REDES DE COMPUTADORAS

NATALIA OLIFER
VICTOR OLIFER



REDES
DE COMPUTADORAS

REDES DE COMPUTADORAS

Principios, tecnología y protocolos para el diseño de redes

Natalia Olifer
Formerly of Moscow State Technical University (MSTU)

Victor Olifer
UK Education and Research Networking Association (UKERNA)

Adaptación y revisión técnica
Jorge Valeriano Assem
División de Ingeniería Eléctrica,
Facultad de Ingeniería,
Universidad Nacional Autónoma de México



MÉXICO • BOGOTÁ • BUENOS AIRES • CARACAS • GUATEMALA
LISBOA • MADRID • NUEVA YORK • SAN JUAN • SANTIAGO
AUCKLAND • LONDRES • MILÁN • MONTREAL • NUEVA DELHI
SAN FRANCISCO • SINGAPUR • SAN LUIS • SIDNEY • TORONTO

Director Higher Education: Miguel Ángel Toledo Castellanos
Director editorial: Ricardo Alejandro del Bosque Alayón
Editor sponsor: Pablo E. Roig Vázquez
Coordinadora editorial: Marcela I. Rocha Martínez
Editor de desarrollo: Edmundo Carlos Zúñiga Gutiérrez
Supervisor de producción: Zeferino García García
Traductores: Carlos Roberto Cordero Pedraza y Efrén Alatorre Miguel
Diseño de portada: Nuria Díaz

REDES DE COMPUTADORAS
Principios, tecnología y protocolos para el diseño de redes



Edificio Punta Santa Fe
Prolongación Paseo de la Reforma 1015, Torre A
Piso 17, Colonia Desarrollo Santa Fe
Delegación Álvaro Obregón
C.P. 01376, México, D. F.
Miembro de la Cámara Nacional de la Industria Editorial Mexicana, Reg. Núm. 736

ISBN: 978-970-10-7249-3

Traducido de la primera edición de: *COMPUTER NETWORKS. Principles, Technologies and Protocols for Network Design*, Published by John Wiley & Sons Ltd. All rights reserved.
Copyright © MMVI.

ISBN: 0-470-86982-8

1234567890 08765432109

Impreso en México *Printed in Mexico*

CONTENIDO

A Klavdia Korytchenko

y

Daniel Ekaette

PREFACIO

ENFOQUE

Este libro representa un curso fundamental acerca de redes de computadoras, el cual combina la cobertura de los temas principales, problemas y tecnologías de esta área del conocimiento en creciente desarrollo, con una consideración a fondo de los detalles de cada tecnología y las características específicas del equipo utilizado. La obra es el resultado de años de experiencia acumulada por los autores a partir de la enseñanza en varias universidades, centros de entrenamiento en empresas comerciales y en grandes firmas corporativas.

Los enunciados siguientes son característicos del presente volumen:

- **Enfoque en las funciones de transporte de la red.** Las funciones de transporte aseguran la transmisión de datos entre computadoras, organizando así una red de computadoras. Se pondrá especial atención en el estudio de la arquitectura de red, los fundamentos principales de la operación del equipo de telecomunicaciones y los protocolos principales, incluido el Protocolo Internet (IP), Ethernet, Bluetooth, IEEE 802.11 (Wi-Fi), el Modo de Transferencia Asíncrona (ATM), Frame Relay, que utilizan las redes para el transporte de datos. Considerando los servicios de red, también se centra el interés en aquellos conceptos dirigidos fundamentalmente al soporte de las funciones de transporte en la red (como el sistema de nombre de dominio, el protocolo de la configuración dinámica del host, VPN e IPSec), más que en proporcionar servicios a los usuarios de computadoras (por ejemplo, servicios Web).

- **No solamente IP.** El éxito de Internet ha hecho de IP el medio principal para construir redes; sin embargo, en este libro no sólo se estudian en detalle las tecnologías IP que permiten la conexión de varias redes disímiles en una superred única (como Internet), sino también se analizan las tecnologías para construir redes, como Ethernet o ATM, con base en las cuales está construida la red unificada. Ambos tipos de tecnologías son igualmente importantes para construir una red eficaz actual y en esta obra se trata de recuperar el balance, el cual se ha sesgado en épocas recientes a favor de IP —un efecto marcado por conocer hacia dónde va la gente—.

- **La combinación de las ciencias de la computación y la ingeniería en computación.** En el presente texto usted encontrará descripciones de los principios de operación de las redes

de telecomunicaciones y los algoritmos de operación de los protocolos de comunicaciones. En general, esta información se clasifica como ciencia de la computación y es necesaria para realizar una investigación exitosa. También se proporcionan un gran número de detalles técnicos acerca de los dispositivos de comunicaciones, así como ejemplos prácticos de diseño de redes de varios tipos. Esto será de mucha utilidad a medida que usted se prepare para practicar la ingeniería, la cual desempeña un papel muy importante para cualquier profesional de las telecomunicaciones.

- **Convergencia de todos los tipos de redes de telecomunicaciones.** La convergencia desempeña un papel cada vez más importante y ejerce una influencia creciente en las redes de computadoras, de televisión y de radio. A partir de los capítulos introductorios de este libro, se refleja esta tendencia actual y se demuestran los principales mecanismos de las redes de computadoras, como el multiplexaje, la conmutación y el enrutamiento, desde las posiciones más generales válidas para las redes de comunicaciones de todo tipo.

A QUIÉN VA DIRIGIDA ESTA OBRA

El material incluido en el presente libro se ha probado con éxito en un público con una actitud sin compromisos. Dicha audiencia estuvo formada por estudiantes con niveles de experiencia e intereses personales considerablemente distintos. Entre ellos hubo estudiantes de licenciatura y posgrado de diferentes universidades, jefes de departamento de tecnologías de información y administradores de red e integradores. Los cursos estuvieron diseñados con el fin de ofrecer una base sólida para un estudio adicional de los principiantes y, al mismo tiempo, para permitir que los especialistas mejoraran y organizaran mejor sus conocimientos.

Dicho libro está dirigido sobre todo a estudiantes de licenciatura y posgrado que deseen obtener conocimientos organizados tanto teóricos como prácticos acerca de las redes de computadoras.

Asimismo, deseamos que el presente volumen sea de utilidad para especialistas que empiecen a estudiar las tecnologías de información y que tengan una idea general solamente acerca de la operación de las redes con base en su trabajo práctico con PC conectadas a Internet. Aquellos que deseen obtener un conocimiento básico pueden utilizar este libro con el fin de continuar su estudio teórico acerca de la operación de las redes.

El libro también será de gran utilidad para profesionales en redes que tengan experiencia, que deseen enterarse de las más nuevas tecnologías y que no hayan encontrado en el curso de sus actividades prácticas y para organizar el conocimiento que ya poseen. Este libro también puede usarse como una referencia práctica en la cual se puedan encontrar la descripción de un protocolo específico, un formato de trama, etc.; además, ofrece las bases teóricas que se requieren para preparar las certificaciones de Cisco, como CCNA, CCNP, CCDP y CCIP.

Este libro está conformado por 21 capítulos organizados en cinco partes, a saber:

- La primera parte, *Fundamentos de la conectividad de redes,* abarca la "primera vuelta" de la espiral cuando se estudian las redes de computadoras. El proceso de aprendizaje siempre tiene una naturaleza espiral. No es factible comprender de inmediato y por completo un fenómeno complejo; por el contrario, cualquier fenómeno de este tipo debe estudiarse desde diferentes puntos de vista, en general y en particular, regresando en ocasiones al estudio de material que en apariencia ya se comprendió y con cada nueva vuelta, la espiral del conocimiento acumula información. En la primera parte, que consiste en siete capítulos, se describen los fundamentos principales y más importantes y las soluciones arquitectónicas, los cuales son la base de todas las tecnologías modernas de redes y que se

estudian en las diferentes partes de este libro. De acuerdo con el proceso de convergencia de redes, se consideraron los principios de conmutación, multiplexaje, enrutamiento y direccionamiento y la arquitectura de las redes de computadoras desde la perspectiva más general, comparadas con los fundamentos similares de otras redes de comunicaciones —redes telefónicas, de transporte, de radio y de televisión—. Esta parte finaliza con el estudio del capítulo que trata acerca de los problemas de la calidad del servicio (QoS) en las redes de conmutación de paquetes. Por lo tanto, los conceptos de QoS considerados por mucho tiempo una rama trivial de las tecnologías de redes se han convertido en uno de los principios básicos en el diseño de las redes de computadoras.

- La segunda parte, *Tecnologías de la capa física*, incluye cuatro capítulos: *8: Enlaces de transmisión; 9: Codificación de datos y multiplexaje; 10: Transmisión inalámbrica, y 11: Redes de transmisión.* Los primeros dos capítulos describen los diferentes tipos de enlaces de transmisión y ofrecen información detallada acerca del método actual para transmitir información discreta a través de las redes. La presencia de este material en el libro permite al lector aprender la cantidad mínima requerida de información sin necesidad de pasar largas horas revisando múltiples publicaciones especializadas. La lista de estas áreas del conocimiento incluye la teoría de la información, el análisis espectral, la codificación de datos física y lógica, y la detección y corrección de errores. En el *capítulo 10* se estudia la transmisión de datos de forma inalámbrica, la cual está siendo más popular cada día. El elevado nivel de ruido y las complejas trayectorias de la propagación de ondas requieren métodos especiales de codificación y transmisión de señales en enlaces de comunicaciones inalámbricos. En el *capítulo 11* se analizan diversas tecnologías, como la jerarquía digital plesiocrona (PDH), SDH/SONET y el multiplexaje por división de onda densa, las cuales forman la infraestructura de los enlaces físicos de las redes globales de telecomunicaciones. Las redes telefónicas o de computadoras instaladas trabajan con base en los canales construidos por las redes de transmisión.

- En la tercera parte, *Redes de área local*, se proporcionan descripciones en detalle de prácticamente todas las tecnologías principales de LAN, incluidas Ethernet, Token Ring y la interfase de datos distribuidos por fibra óptica (FDDI), así como tecnologías de alta velocidad más modernas. Existen LAN actuales cuando domina una de las tecnologías o, para ser más precisos, la familia de tecnologías —Ethernet—. Naturalmente, se examina esta tecnología con más profundidad que las otras. En el *capítulo 12* se estudia la tecnología Ethernet a 10 Mbps clásica, y en el *capítulo 13* se describen las versiones a alta velocidad de Ethernet con base en el medio compartido, llámese Fast Ethernet o Gigabit Ethernet. En el *capítulo 14* se describen otras tecnologías LAN que también utilizan un medio compartido —Token Ring, FDDI y dos tecnologías inalámbricas—, la LAN IEEE 802.11 y la red de área personal Bluetooth. Los dos últimos capítulos de esta parte, *15 y 16,* están dedicados a las LAN conmutadas. En el primero se estudian los principios fundamentales de la operación de dichas redes: el algoritmo de la operación del switch LAN, las versiones dúplex de los protocolos LAN y las características específicas de la implementación de los switches LAN. En el *capítulo 16* se analizan las potencialidades adicionales de las redes de este tipo, incluidos los enlaces de respaldo en el algoritmo de árbol extendido y la técnica de LAN virtual.

- De acuerdo con la lógica que establece el modelo de interconexión de sistemas abiertos, las partes dedicadas a las tecnologías de las capas física y de enlace de datos deben ser examinadas en la cuarta *parte,* que se concentra en las tecnologías de la capa de red que aseguran la posibilidad de combinar un gran número de redes diferentes en una red

unificada. Debido a que IP es el líder indiscutible entre los protocolos de la capa de red, le dedicamos gran parte de nuestra atención en este libro. En el *capítulo 17* se explican diferentes aspectos del direccionamiento IP: los métodos de mapeo de direcciones locales, de red y simbólicas; los métodos para usar las máscaras de red; los métodos modernos para agregar direcciones IP; y los métodos de configuración automática de los nodos IP. En el *capítulo 18* se estudia en detalle la operación de IP en relación con el direccionamiento y fragmentación de paquetes, se describe el formato general de la tabla de enrutamiento y se dan ejemplos de su implementación particular en ruteadores de hardware y software de diferentes tipos. En la descripción de las características específicas de la nueva versión de IP —IPv6— se estudió el método de modernización del direccionamiento en detalle, así como los principales cambios realizados al formato del encabezado IP. El *capítulo 19* comienza con el estudio del protocolo de control de la transmisión (TCP) y el protocolo del datagrama de usuario (UDP), los cuales desempeñan un papel de intermediarios entre las aplicaciones y la infraestructura de transporte de la red. Más adelante, se estudia el protocolo de información de enrutamiento (RIP), la primera trayectoria abierta más corta (OSPF) y el protocolo de puerta de enlace (Gateway) fronteriza (BGP). Con el material que se proporciona se pueden analizar las áreas de aplicación de estos protocolos y la posibilidad de su uso en conjunto. Se concluye el capítulo con el estudio del protocolo de mensaje de control de Internet, que es la manera de informar al emisor por qué sus paquetes no fueron entregados al nodo destino. En el *capítulo 20* se describen los tipos y características principales de los ruteadores, las variantes de su organización interna y los métodos para combinar las funciones de conmutación en enrutamiento dentro del mismo dispositivo: el switch de la capa 3. La investigación minuciosa del conjunto de protocolos TCP/IP en la *parte IV* lo hace muy valioso como una introducción independiente a las redes IP.

- *Quinta parte: Las redes de área amplia.* La tecnología IP considerada en la parte anterior de este libro permite construir redes de diferentes tipos tanto locales como globales; además, existen otras tecnologías basadas en la técnica del circuito virtual que se diseñaron especialmente para las WAN. Estas tecnologías, implantadas en redes Frame Relay y ATM, se estudian en el *capítulo 21*. La técnica del circuito virtual representa una alternativa al método del datagrama del direccionamiento de paquetes, el cual es la base de las redes Ethernet e IP. La competencia entre estos dos principios fundamentales de transmisión de datos ha existido por mucho tiempo, prácticamente a partir del comienzo del desarrollo de las redes de conmutación en paquetes.

  Si bien es cierto que el estudio de las WAN puede extenderse mucho más aún, se considera que ello va más allá de los alcances propuestos por este libro. No obstante, para los lectores interesados en profundizar en el tema, se ofrecen una serie de lecturas recomendadas para todos los temas (inclusive las redes de área amplia) al final del libro.

Hemos puesto todo nuestro esfuerzo con el fin de que el trabajo del lector con este libro sea lo más eficiente posible. El índice detallado le permitirá encontrar, de manera rápida, el material de su interés utilizando los múltiples términos que existen en la industria de las redes actual. Cada capítulo cuenta con una sección de resumen que facilita al lector concentrarse en las ideas principales, en los temas y en los resultados de determinado capítulo. Lo anterior le ayudará a evitar la omisión de los principios fundamentales debido a la abundancia de hechos y detalles. Por último, cada capítulo termina con preguntas y problemas de repaso que se diseñaron con el fin de verificar el nivel de conocimiento que se obtuvo como resultado de la lectura de ese capítulo. En algunos casos, estos problemas tienen un significado especial debido a que le ayudan a comprender mejor ciertas ideas.

AGRADECIMIENTOS

Estamos profundamente agradecidos con los empleados de John Wiley & Sons, que elaboraron la edición en inglés: Gaynor Redvers-Mutton, editor en jefe del programa de libros sobre ciencias de la computación; Jonathan Shipley, editor asociado del programa de libros sobre ciencias de la computación; Sarah Corney, editora ejecutiva de proyecto del grupo de educación superior; y David Barnard, editor de proyecto. Asimismo, apreciamos el trabajo de los empleados de las casas editoras A-List y BHV, en particular de Vadim Sergeev, Natalia Tarkova, Olga Kokoreva y Julie Laing. Con su ayuda nuestro libro, el cual va en su tercera edición en Rusia, se encuentra disponible en el idioma inglés; todos ellos también ayudaron significativamente a mejorar la versión inicial del libro. Hacemos público nuestro especial agradecimiento a Alexey Jdanov, editor de la edición rusa, cuyos comentarios fueron muy valiosos para depurar la calidad de esta obra.

Victor y Natalia Olifer

PARTE I

FUNDAMENTOS DE LA INTERCONECTIVIDAD DE REDES

El proceso de adquisición de conocimiento siempre es de naturaleza espiral elíptica. Resulta imposible comprender y apreciar de manera inmediata un fenómeno intrincado. Para percibirlo de manera adecuada, debemos considerar dicho fenómeno desde diferentes puntos de vista y observarlo como un todo así como en sus partes, de forma separada y en relación con otro fenómeno, acumulando nuestro conocimiento gradualmente. Además, de vez en cuando es necesario reconsiderar los conceptos que en apariencia ya se habían comprendido, de tal modo que tengamos en cada vuelta de la espiral una mejor idea de la naturaleza de ese fenómeno. Un buen método consiste en estudiar inicialmente los principios generales más importantes de las áreas de conocimiento específicas, seguido de una investigación minuciosa acerca de cómo se implementan estos principios en métodos, tecnologías o estructuras específicos.

La parte introductoria de este libro representa la primera parte de la espiral en el estudio de las redes de computadoras. Describe los fundamentos principales y las soluciones arquitectónicas que constituyen la base de todas las tecnologías contemporáneas de conectividad de redes que se estudiarán en secciones posteriores de este libro. De acuerdo con el concepto de convergencia de redes, trataremos de explicar los fundamentos de la conmutación, el multiplexaje, el enrutamiento, el direccionamiento y la arquitectura de redes desde el punto de vista más básico y general. Para hacer esto, debemos comparar los fundamentos de las redes de computadoras con los correspondientes de otras redes de comunicaciones, como las telefónicas, las de transmisión, las de radio y las de televisión.

En el último capítulo de esta parte se estudian los problemas asociados con la calidad de servicio (QoS, por sus siglas en inglés) en redes de conmutación de paquetes. El nuevo papel que desempeñan las redes de computadoras como la base para el desarrollo de las redes públicas de nueva generación capaces de proporcionar toda clase de servicios de información y transmisión de datos, voz y video ha dado como consecuencia la adopción de los métodos de evaluación de la calidad del servicio en prácticamente todas las tecnologías de comunicación. Por tanto, los conceptos relacionados con QoS, que durante mucho tiempo se consideraron un área especializada y avanzada de las tecnologías de redes, se han convertido en uno de los conceptos fundamentales utilizados en el diseño de las redes de computadoras.

Después de estudiar minuciosamente las tecnologías específicas, será de utilidad (y de interés, esperan los autores) regresar a la primera parte del libro. Esta nueva iteración del proceso de aprendizaje permitirá que el lector comprenda mejor los principios básicos de operación de las redes de computadoras y de la implementación de estos principios en diferentes tecnologías.

La parte I abarca los capítulos siguientes:

- Capítulo 1: Evolución de las redes de computadoras.
- Capítulo 2: Principios generales del diseño de redes.
- Capítulo 3: Conmutación de circuitos y de paquetes.
- Capítulo 4: Arquitectura y estandarización de redes.
- Capítulo 5: Ejemplos de redes.
- Capítulo 6: Características de las redes.
- Capítulo 7: Métodos para asegurar la calidad del servicio.

1 EVOLUCIÓN DE LAS REDES DE COMPUTADORAS

DESCRIPCIÓN DEL CAPÍTULO

1.1 INTRODUCCIÓN

El estudio de la evolución de cualquier área de la ciencia o de la tecnología no solamente estimulará su curiosidad natural, sino también le permitirá comprender más a fondo los principales logros en dicha área, lo concientizará de las tendencias actuales y le ayudará a evaluar los prospectos de los desarrollos específicos. Las redes de computadoras aparecieron en fechas recientes, a finales de los años de 1960 y han heredado un gran número de propiedades útiles de sus predecesores, las viejas y ampliamente difundidas redes telefónicas. Esto no es una sorpresa, ya que tanto los teléfonos como las computadoras son instrumentos universales de comunicación.

Sin embargo, las redes de computadoras han aportado algo novedoso al mundo de las comunicaciones: el prácticamente inagotable almacenamiento de información acumulada por la civilización humana en el transcurso de sus varios miles de años de existencia. Este almacenamiento de información continua crece de manera constante. Lo anterior fue particularmente notable a mediados de la década de 1990, cuando el rápido crecimiento de Internet demostró claramente que el acceso libre y anónimo a la información y las comunicaciones instantáneas y por escrito era de gran valor para la mayoría de las personas.

La influencia de las redes de computadoras en otros tipos de redes dio como resultado la convergencia de redes, un proceso que comenzó mucho antes que Internet. La transmisión de voz digital a través de las redes telefónicas fue uno de los primeros indicios de dicha convergencia. Indicios más recientes de la convergencia son constituidos por el desarrollo activo de nuevos servicios en redes de computadoras que eran privativos de las redes telefónicas, de radio y de televisión, como voz sobre IP (VoIP), transmisiones por radio y servicios de televisión. El proceso de convergencia es continuo, aunque no ofrece signos claros acerca de su futuro; sin embargo, el conocimiento de la evolución de las redes de computadoras, que se describe en este capítulo, permite comprender de manera más sencilla los principales problemas a los que se deben enfrentar los diseñadores de las redes de computadoras.

1.2 ANTECEDENTES DE LAS REDES DE COMPUTADORAS

PALABRAS CLAVE: *mainframe*, sistemas de procesamiento por lotes, sistemas de procesamiento por tiempo compartido, sistemas multiterminales, red de computadoras o red de transmisión de datos, Ley de Grosch, redes de area local (LAN), tecnologías LAN estándar: Ethernet, Arcnet, *Token Ring*, FDDI.

1.2.1 Las redes de computadoras como resultado de la evolución de las tecnologías de cómputo y de las comunicaciones

Las **redes de computadoras** que se estudian en este libro no son el único tipo de redes que la civilización humana haya creado. Es posible que el ejemplo más antiguo de una red que haya abarcado grandes territorios y ofrecido servicios a múltiples clientes haya sido el sistema de suministro de agua en la antigua Roma. Pero, sin importar qué tan distantes y diversas en su naturaleza puedan ser las redes, todas tienen algo en común. Por ejemplo, se puede dibujar una analogía clara entre los componentes de las redes eléctricas y los de cualquier red de computadoras de gran tamaño. Es decir, los recursos de información que se encuentran en las redes de computadoras corresponden a las plantas de energía eléctrica; los enlaces de comunicación de las redes de computadoras son análogos a las líneas de transmisión de alta

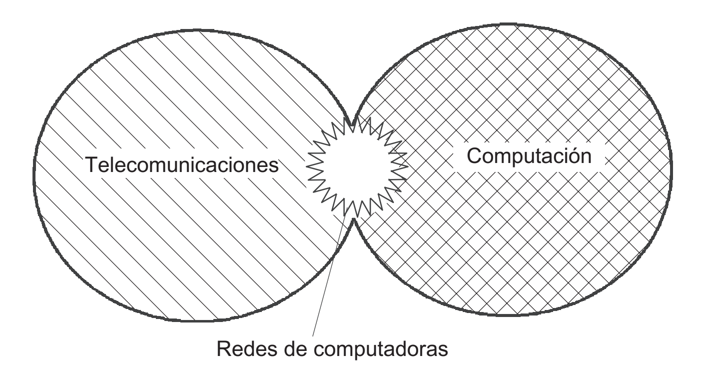


FIGURA 1.1 Evolución de las redes de computadoras en la interfase entre las tecnologías de la computación y de las telecomunicaciones.

tensión y las redes de acceso son parecidas a las estaciones de transformación. Por último, tanto en las redes de computadoras como en las eléctricas se puede observar que cuentan con terminales para los clientes: estaciones de trabajo del usuario final en el caso de las redes de computadoras y aparatos eléctricos domésticos en el caso de las redes eléctricas.

Las redes de computadoras, también conocidas como **redes de comunicación de datos** o **de transmisión de datos**, representan el resultado lógico de la evolución de dos de las ramas científicas y tecnológicas más importantes de la civilización moderna: las tecnologías de las computadoras y de las telecomunicaciones.

Por un lado (figura 1.1), las redes de computadoras representan un caso particular de sistemas de cómputo distribuido en los que un grupo de computadoras trabajan de manera coordinada para realizar una serie de tareas interrelacionadas mediante el intercambio de datos de manera automática. Las redes de computadoras también pueden considerarse como un medio de transmitir información a larga distancia. Para hacer lo anterior, las redes de computadoras implementan varios métodos para codificar y multiplexar datos, los cuales han sido adoptados ampliamente por los sistemas de telecomunicaciones.

1.2.2 Sistemas de procesamiento por lotes

En primera instancia, considere los orígenes de las redes de computadoras. Las computadoras de la década de 1950 —enormes, voluminosas y caras— se diseñaron para un pequeño número de usuarios privilegiados. Con mucha frecuencia, estos monstruosos equipos ocupaban edificios completos. Dichas computadoras no podían prestar servicio a los usuarios de manera interactiva, por lo que primero formaban lotes de tareas y después entregaban los resultados.

Los **sistemas de procesamiento por lotes** estaban basados primordialmente en *mainframes* y constituían computadoras universales poderosas y confiables. Los usuarios preparaban tarjetas perforadas que contenían datos y códigos de programa y después transferían estas tarjetas al centro de cómputo. Los operadores insertaban estas tarjetas a la computadora y los usuarios obtenían los resultados un día después en forma impresa (figura 1.2). Por tanto, una sola tarjeta perforada que tuviera un error podría significar un retraso de al menos 24 horas.

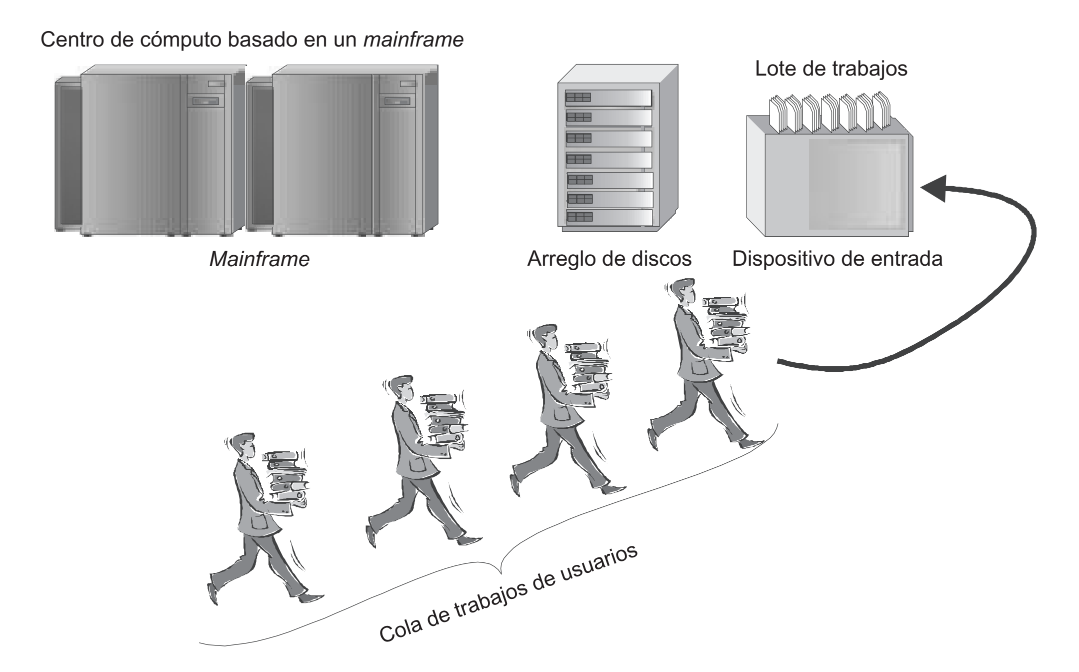


FIGURA 1.2 Sistema centralizado basado en un *mainframe*.

Como era obvio, desde el punto de vista del usuario final, sería más conveniente contar con un modo de operación interactivo que les permitiera manejar el procesamiento de sus datos de una sola vez desde la terminal. Los intereses de los usuarios finales fueron omitidos totalmente en las primeras etapas de la evolución de los sistemas de computadoras. La eficiencia del desempeño del componente más costoso de una computadora —el procesador— se consideró de fundamental importancia, aun a costa de la productividad del usuario.

1.2.3 Sistemas multiterminales: prototipo de una red de computadoras

A medida que los procesadores se abarataron a principios de la década de 1960, aparecieron nuevos métodos para diseñar el procesamiento en las computadoras. Dichos métodos vislumbraron la posibilidad de tener en cuenta la conveniencia del usuario final. Por tanto, los sistemas multiterminales evolucionaron (figura 1.3). En dichos sistemas de tiempo compartido, la computadora estaba a disposición de varios usuarios, quienes tenían sus propias terminales, desde donde podían comunicarse con la computadora. El tiempo de respuesta del sistema de cómputo era lo suficientemente corto para ocultar que la computadora daba servicios a múltiples usuarios en paralelo.

Las terminales podían instalarse fuera de los centros de cómputo y sobre los escritorios de todas las empresas. A pesar de que el poder de procesamiento se conservaba totalmente centralizado, algunas funciones se distribuyeron, como la entrada y salida de datos. Dichos sistemas multiterminales centralizados tenían una apariencia similar a las Redes de Área Local (LAN, por sus siglas en inglés). Los usuarios finales percibían el funcionamiento en una terminal prácticamente de la misma manera que en la actualidad la mayoría de la gente percibe el funcionamiento de una PC conectada a una red. El usuario podía acceder a los archivos y dispositivos periféricos compartidos y tener la impresión de usar la computadora de manera exclusiva, pues el usuario podía iniciar cualquier programa que deseara en cual-

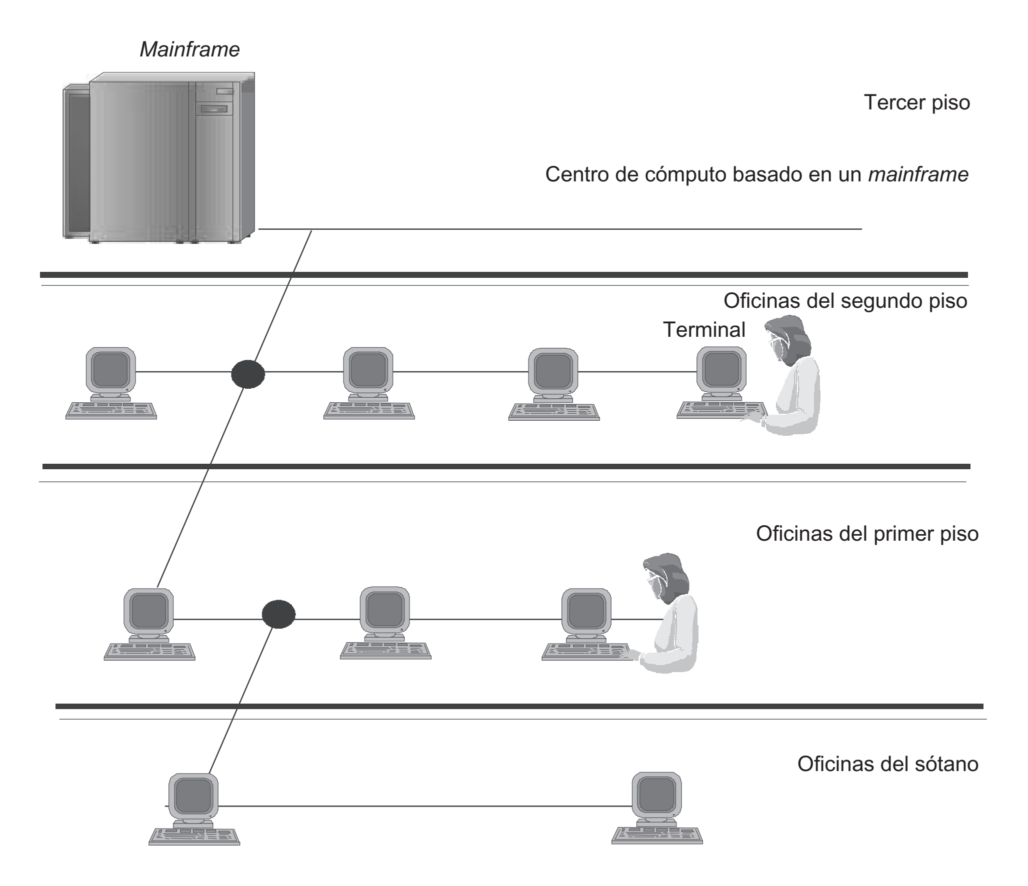


FIGURA 1.3 Sistema multiterminal como prototipo de una red de computadoras.

quier momento y recibir los resultados casi de forma inmediata. (Algunos usuarios estaban convencidos de que las operaciones matemáticas se llevaban a cabo en alguna parte dentro de la pantalla de la computadora.)

> Los sistemas multiterminales, los cuales trabajaban en modo de tiempo compartido, fueron el primer paso en el desarrollo de las LAN.

Sin embargo, la evolución aún tuvo que recorrer un largo camino antes de que aparecieran las LAN, ya que los sistemas multiterminales conservaron las características esenciales del procesamiento centralizado de datos, a pesar de su somero parecido con los sistemas distribuidos.

Los corporativos consideraban que no había una necesidad imperiosa de las LAN. En un solo edificio no había nada que conectar como para utilizar una red. La mayoría de las empresas no podía darse el lujo de comprar más de una computadora. Durante ese periodo, la famosa *ley de Grosch* (nombrada así en honor a Herbert Grosch) fue universalmente válida y representaba, de manera empírica, el nivel tecnológico de ese entonces. De acuerdo con esta ley, el costo de un sistema de cómputo se elevaba en función de la raíz cuadrada del poder computacional del sistema. De aquí que era económicamente más provechoso comprar una máquina poderosa que dos menos poderosas, porque su poder computacional total resultaba significativamente menor que el de la máquina más costosa.

1.3 PRIMERAS REDES DE COMPUTADORAS

PALABRAS CLAVE: conmutación en paquetes, tráfico en ráfagas, red de área amplia (WAN), tecnología de la red telefónica, troncal, redes de transmisión, paquete, Internet, sistema operativo de red, tecnologías estándares de LAN: Ethernet, Arcnet, *Token Ring* y FDDI.

1.3.1 Primeras redes de área amplia (WAN)

En contraste, era inminente la necesidad de conectar computadoras ubicadas a grandes distancias entre sí. Todo comenzó con la solución de una tarea muy simple; es decir, proporcionar acceso a una computadora desde terminales remotas ubicadas a cientos o, a veces, a miles de kilómetros de distancia. Los módem se utilizaron para conectar terminales a computadoras mediante el uso de líneas telefónicas. Dichas redes permitieron que múltiples usuarios remotos pudieran acceder a los recursos compartidos de varias supercomputadoras poderosas. Cuando aparecieron los sistemas distribuidos se implantaron conexiones no sólo entre *terminales* y *computadoras*, sino también entre *computadoras*.

Las computadoras fueron capaces de intercambiar datos en forma automática, lo cual, en esencia, es el mecanismo fundamental de cualquier red de computadoras. Los diseñadores de las primeras redes implantaron servicios para el intercambio de archivos, la sincronización de bases de datos, el correo electrónico y otros servicios de la red que son utilizados en la actualidad.

Desde el punto de vista cronológico, las **redes de área amplia (WAN)** fueron las primeras en aparecer y conectaban computadoras distribuidas geográficamente e incluso aquellas localizadas en diferentes ciudades y países.

Durante el proceso de desarrollo de las WAN aparecieron y se desarrollaron muchas ideas fundamentales de las redes modernas de computadoras, como las siguientes:

- Arquitectura multicapa de los protocolos de comunicación
- Tecnología de conmutación de paquetes
- Enrutamiento de paquetes en redes heterogéneas

A pesar de que las WAN heredaron muchas características de las redes antiguas, de largo alcance y de uso muy diseminado como las **redes telefónicas**, la característica más innovadora fue la de alejarse del principio de la conmutación de circuitos, el cual por décadas había sido utilizado con éxito en las redes telefónicas.

Un circuito con una velocidad constante asignado a una sesión no podría emplearse de forma eficaz con el **tráfico en ráfagas**[1] de los datos de una computadora (en ráfagas significa que se alternan periodos de intenso intercambio de datos con pausas largas). Tanto experimentos como modelos matemáticos han demostrado que las redes basadas en el principio de conmutación en paquetes pueden transmitir tráfico en ráfagas de manera más eficaz.

---

[1] Los términos *ráfaga* y *tráfico en ráfagas* son reconocidos y comúnmente adoptados en el campo de la comunicación de datos. De acuerdo con las definiciones técnicas proporcionadas por Cisco Systems, ráfaga es una secuencia de señales que se cuentan como una unidad de acuerdo con algún criterio o medida específicos, mientras que el término tráfico en ráfagas se refiere a un patrón irregular de transmisión de datos.

De acuerdo con el principio de **conmutación en paquetes**, los datos se dividen en pequeños fragmentos conocidos como **paquetes**. La dirección de destino del *host* se encuentra incluida en el encabezado del paquete, permitiendo así que cada paquete viaje a través de la red por sí mismo.

Como la construcción de líneas de comunicaciones de alta calidad que conectan lugares distantes es muy costosa, a menudo las primeras WAN utilizaban enlaces de comunicaciones disponibles que originalmente se diseñaron con diversos propósitos. Por ejemplo, por mucho tiempo las WAN se construyeron con base en las líneas telefónicas. Debido a que la velocidad de transmisión de los datos discretos de las computadoras que usaban dichos enlaces era muy baja, cientos de kilobits por segundo (Kbps), el conjunto de servicios proporcionados por dichas redes estaba limitado a la transferencia de archivos, principalmente en modo de segundo plano y al correo electrónico. Además de la baja velocidad de transmisión, dichos canales tenían otra desventaja: introducían distorsiones significativas a las señales transmitidas. Por tanto, los protocolos de red en las WAN que utilizaban líneas de comunicación de baja calidad estaban caracterizados por procedimientos complejos para el control y el restablecimiento de datos. Un ejemplo típico de este tipo de redes es la X.25, diseñada a principios de la década de 1970, cuando prevalecía el uso de canales analógicos arrendados de las compañías telefónicas para conectar las computadoras y switches de las WAN.

En 1969, el Departamento de Defensa de Estados Unidos comenzó a investigar acerca de la conexión de las computadoras de los centros militares y de investigación en una red. Dicha red, la cual se conoció con el nombre de **ARPANET**, sirvió como punto de partida para la construcción de la primera y más popular WAN, conocida en la actualidad con el nombre de **Internet**.

ARPANET conectaba computadoras de diferentes tipos, corriendo según distintos sistemas operativos con varios módulos que se podían adicionar mediante la implementación de protocolos de comunicación comunes a todas las computadoras que formaban parte de la red. Dichos sistemas operativos pueden considerarse en realidad los primeros **sistemas operativos de red**.

Los sistemas operativos de red, en contraste con los multiterminales, permitieron que el sistema no solamente distribuyera usuarios, sino también organizara el almacenamiento de datos. Dichos sistemas también hicieron factible que el procesamiento se distribuyera entre varias computadoras conectadas mediante enlaces eléctricos. Cualquier sistema operativo de red es capaz de llevar a cabo todas las funciones de un sistema operativo local y de proporcionar funciones adicionales, permitiendo así que el sistema se pueda comunicar con otros sistemas operativos por medio de la red. Los módulos de software, que implementan funciones para la conectividad de redes, fueron incorporados en los sistemas operativos de manera gradual, con avances en tecnologías de red y hardware de computadoras, a medida que aparecieron nuevas tareas que requerían procesamiento de red.

El avance tecnológico de las WAN dependió sobre todo del correspondiente de las redes telefónicas.

> Desde finales de la década de 1960, la transmisión de voz en formato digital se convirtió en algo muy común en las redes telefónicas.

Lo anterior resultó en la aparición de canales digitales de alta velocidad que conectaban centrales telefónicas automáticas y permitían la transmisión simultánea de decenas o incluso cientos de conversaciones. Se desarrolló tecnología especial para construir **redes de transmisión** o **troncales (backbones)**. Dichas redes no prestan servicio a usuarios finales, sino que

representan la base en la que están construidos los canales digitales punto-a-punto de alta velocidad. Estos canales conectan el equipo de otra red (la red superpuesta) que proporciona servicios a los usuarios finales.

Al principio, las redes de transmisión representaban exclusivamente tecnología interna que sólo utilizaban las compañías telefónicas; sin embargo, de manera gradual, dichas compañías comenzaron a arrendar parte de sus canales digitales conectados a redes de transmisión a compañías que los usaron para formar sus propias redes telefónicas y WAN. En la actualidad, las redes de transmisión han aumentado su velocidad de transmisión de datos a cientos de gigabits por segundo (Gbps) y, en algunos casos, a varios terabits por segundo; dichas redes abarcan los territorios de los principales estados industriales.

Tanto la variedad como la calidad de servicios han ayudado a que las WAN sean equivalentes a las LAN, las cuales habían sido las líderes a pesar de su relativamente reciente aparición.

1.3.2 Primeras redes de área local (LAN)

A principios de la década de 1970 se llevó a cabo un evento que ha tenido la mayor influencia en la evolución de las redes de computadoras. Como resultado de los avances tecnológicos en el campo de la fabricación de componentes para computadora, aparecieron circuitos integrados de gran escala (dispositivos LSI). Estos dispositivos estaban caracterizados por un costo relativamente bajo, así como por funciones avanzadas. Lo anterior llevó al desarrollo de minicomputadoras, las cuales se convirtieron en los verdaderos competidores de los *mainframes*. La ley de Grosch dejó de ser válida, pues una docena de minicomputadoras que tuvieran el mismo costo que un *mainframe* podía efectuar algunas tareas (especialmente las que podían realizarse en paralelo) mucho más rápido.

A partir de ese momento, aun pequeñas compañías pudieron darse el lujo de tener sus computadoras. Las minicomputadoras podían llevar a cabo tareas como el control de equipo técnico y la administración de las existencias en dichas compañías. Esto representó el origen del concepto de cómputo distribuido, en el que los recursos de cómputo estaban distribuidos por toda la compañía, sin embargo, todas las computadoras en la misma organización continuaron trabajando en forma independiente (figura 1.4).

A medida que transcurrió el tiempo, las necesidades de los usuarios evolucionaron. Los usuarios finales ya no estaban satisfechos del trabajo aislado en una computadora independiente, por ejemplo: necesitaban intercambiar datos de computadora (a menudo, de manera automática) con los usuarios de sus demás sucursales y oficinas. Con el fin de satisfacer estas necesidades, aparecieron las primeras LAN (figura 1.5).

Las LAN representan grupos de computadoras concentradas en una región relativamente pequeña, por lo general dentro de un radio que no excede de 2.5 kilómetros, aunque las LAN pueden extenderse para abarcar áreas mayores (docenas de kilómetros). En general, las LAN representan un sistema de comunicación que pertenece a una sola organización.

Al principio se utilizaron *tecnologías no estándares* para la interconectividad de redes con el fin de conectar computadoras a la red.

La **tecnología de redes** es un conjunto coordinado de software y hardware (por ejemplo, controladores, adaptadores de red, cables y conectores) y mecanismos para la transmisión de datos a través de enlaces de comunicación, suficientes para construir una red de computadoras.

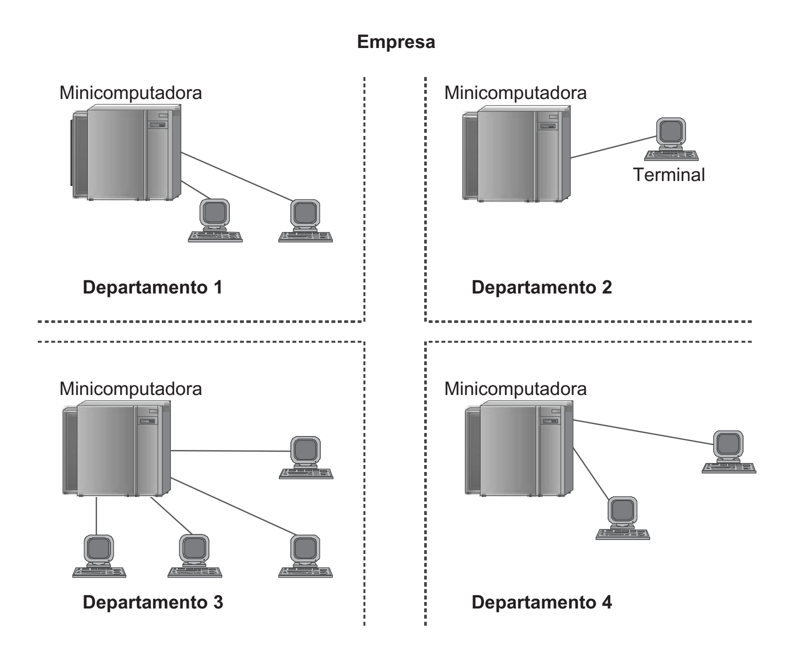


FIGURA 1.4 Operación independiente de varias minicomputadoras ubicadas en la misma empresa.

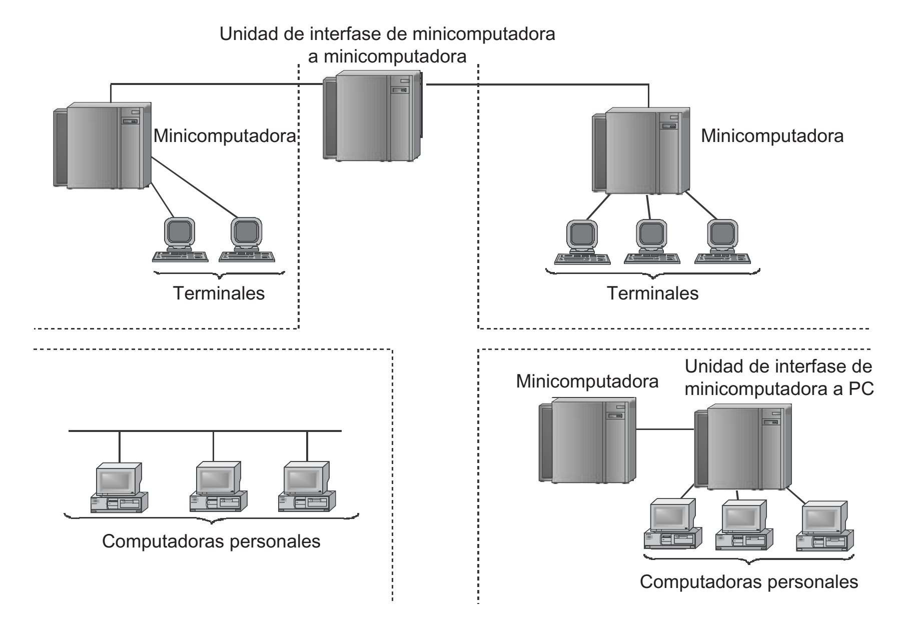


FIGURA 1.5 Tipos de enlaces en las primeras LAN.

Varias unidades de interfase propietarias que utilizaban técnicas propietarias para representar datos en los enlaces de comunicaciones, tipos de cable propietarios, etc., podían conectar tipos y modelos de computadoras específicos, para los cuales estaban diseñados. Algunos ejemplos son las interfases para conectar minicomputadoras PDP-11 con *mainframes* IBM 360 o minicomputadoras Hewlett-Packard con microcomputadoras LSI-11.

A mediados de la década de 1980, la situación comenzó a cambiar en forma radical. Las **tecnologías estándar** para conectar computadoras a la red, como Ethernet, Arcnet, *Token Ring* y poco después FDDI, se establecieron permanentemente.

La adopción de las computadoras personales representó un incentivo muy poderoso para el desarrollo de estas tecnologías. Las PC se convirtieron en elementos ideales en la construcción de redes: por un lado, eran lo suficientemente poderosas para soportar software para la conectividad de redes; por otro, era obvio que necesitaban conectar sus capacidades de procesamiento con el fin de resolver tareas complejas y compartir dispositivos periféricos costosos y arreglos de discos. Debido a lo anterior, las PC prevalecieron en las LAN no sólo jugando el rol de clientes, sino también llevando a cabo funciones de almacenamiento de datos y de central de procesamiento (es decir, convirtiéndose en servidores de red). A medida que las PC fueron más populares, absorbieron las funciones que normalmente realizaban las minicomputadoras y las *mainframes*.

Todas las tecnologías estándares de LAN estaban basadas en el mismo principio de conmutación que era muy exitoso cuando se transmitía tráfico a través de las WAN, es decir, el principio de la conmutación de paquetes.

El proceso para diseñar LAN pasó de ser de un trabajo artesanal a un procedimiento estándar mediante el uso de tecnologías para la conectividad de redes. Para construir una red, era suficiente comprar un cable estándar y adaptadores de red de acuerdo con la especificación requerida (por ejemplo, Ethernet), conectar adaptadores al cable utilizando conectores estándar e instalar en la computadora algunos de los sistemas operativos de red populares en esa época (NetWare de Novell, por ejemplo).

Los diseñadores de LAN introdujeron muchas innovaciones que afectaron la organización del trabajo del usuario final. Tareas como el acceso a los recursos compartidos de la red fueron significativamente más sencillas. En contraste con los usuarios de las WAN, la gente que utilizaba las LAN se liberó de la necesidad de memorizar complejos identificadores de recursos compartidos. Para tal propósito, el sistema ofrecía la lista de recursos disponibles en un formato amigable al usuario (por ejemplo, en una estructura jerárquica tipo árbol). Otra ventaja de trabajar con LAN era que, después de establecer la conexión con el recurso remoto, la gente podía acceder a dicho recurso utilizando los mismos comandos que empleó cuando trabajó con recursos locales. La aparición de un gran número de usuarios finales liberados de estudiar los comandos especializados (y muy complejos) para la conectividad de redes fue la consecuencia, así como la causa, de dicho progreso.

Así, surge la pregunta: ¿por qué todas estas ventajas estuvieron disponibles a los usuarios finales solamente hasta que aparecieron las LAN? Principalmente, debido a que las LAN utilizan cableado de alta calidad. Aun los adaptadores de red de primera generación aseguraban una velocidad de transferencia de datos de hasta 10 Mbps. Como las LAN están caracterizadas por su cobertura limitada, el costo de dichos enlaces fue manejable. Por esta razón, economizar en el ancho de banda, un aspecto importante de las tecnologías WAN anteriores, no representaba un problema significativo en el desarrollo de protocolos para LAN. En estas condiciones, la difusión periódica de recursos y servicios del servidor se convirtió en el mecanismo principal para la organización del acceso transparente a los recursos de las LAN. Con base en esta difusión, las computadoras cliente hicieron listas de los recursos disponibles de red y las presentaron a los usuarios.

TABLA 1.1 Cronología de los eventos más significativos en la historia de las redes de computadoras

Primeras conexiones globales entre computadoras. Primeros experimentos con redes que utilizaban procesamiento en lotes.	Finales de la década de 1960
Comienzo de la transmisión digital de voz a través de redes telefónicas.	Finales de la década de 1960
Llegada de los circuitos integrados a gran escala. Primeras minicomputadoras. Primeras LAN propietarias.	Principios de la década de 1970
Desarrollo de la arquitectura de red de sistemas IBM.	1974
Estandarización de la tecnología X.25.	1974
Llegada de las primeras computadoras personales.	Principios de la década de 1980
Creación de Internet en su forma actual. Instalación de la pila de protocolos TCP/IP en todos los nodos.	Principios de la década de 1980
Llegada de las primeras tecnologías estándares de LAN.	Ethernet: 1980 *Token Ring*: 1985 FDDI: 1985
Comienzo del uso comercial de Internet.	Finales de la década de 1980
Invención de la Telaraña Mundial de la Información.	1991

A finales de la década de 1990, la familia Ethernet se convirtió en el líder indiscutible de las tecnologías LAN. Además de la tecnología Ethernet clásica (10 Mbps), esta familia incluía Fast Ethernet (100 Mbps) y Gigabit Ethernet (1 000 Mbps).

El uso de algoritmos simples aseguró el bajo costo del equipo Ethernet. La gama de velocidades de transmisión de datos hizo posible que los arquitectos de red utilizaran un método racional en el momento de diseñar LAN y seleccionaran la tecnología Ethernet específica que mejor se adecuara a las necesidades de la empresa. Todas las tecnologías de Ethernet guardan cierto parecido entre sí en cuanto a sus principios de operación, su simplificado mantenimiento y su integración.

La secuencia cronológica de los acontecimientos más significativos en la historia de la evolución de las redes de computadoras se muestra en la tabla 1.1.

1.4 CONVERGENCIA DE LAS REDES

PALABRAS CLAVE: convergencia, intranet, Internet, redes de área metropolitana (MAN), redes de multiservicio, redes de telecomunicaciones, redes de datos, tecnologías estándares para la interconectividad de redes, FDDI, Ethernet, *Token Ring*, ATM, red digital de servicios integrados (ISDN) y conectividad de redes, QoS.

1.4.1 Convergencia de LAN y WAN

A finales de la década de 1980 eran evidentes las siguientes diferencias entre LAN y WAN:

- *Longitud y calidad de los enlaces de comunicación.* Las LAN se distinguían de las WAN por sus distancias moderadas entre los nodos de la red. Principalmente, este factor permitió a los diseñadores de redes utilizar enlaces de comunicaciones de mejor calidad que en las WAN.
- *Complejidad de los métodos de transmisión de datos.* Debido a la baja confiabilidad de los canales físicos de comunicación, las WAN requieren métodos más sofisticados para la transmisión de datos, así como equipo más complejo que las LAN.
- *Velocidad de comunicación de datos.* En las LAN, las velocidades (10, 16 y 100 Mbps) eran significativamente más elevadas que en las WAN (de 2.4 Kbps a 2 Mbps).
- *Gama de servicios.* Las elevadas transferencias de datos hacen posible que los diseñadores de red puedan implantar una gran variedad de servicios en las LAN. Entre dichos servicios está la amplia capacidad de acceso y de utilizar archivos almacenados en los discos duros de otras computadoras conectadas en red; compartir dispositivos de impresión, módems y faxes; acceder a bases de datos centralizadas, y usar el correo electrónico. La gama de servicios proporcionados por las WAN estaba limitada primordialmente a servicios de correo y archivos en sus formas más simples (las cuales no eran las más convenientes para la mayoría de los usuarios).

De manera gradual, las diferencias entre las LAN y las WAN comenzaron a desaparecer. Los diseñadores de red empezaron a conectar LAN aisladas, utilizando WAN como medio de conexión. La gran integración entre LAN y WAN dio como resultado la penetración significativa de las tecnologías adecuadas.

La convergencia de los métodos de transmisión de datos está basada en la plataforma de la transmisión de datos digital a lo largo de las líneas de comunicación de fibra óptica. Este medio de transmisión se utiliza en prácticamente todas las tecnologías LAN que buscan un intercambio de datos a alta velocidad en distancias mayores que 110 yardas. Este medio de transmisión se utiliza como base en todos los enlaces troncales de las redes de transmisión actuales, que proveen canales digitales para conectar equipo WAN.

La alta calidad de los enlaces digitales ha modificado los requerimientos de los protocolos WAN. En lugar de procedimientos que aseguren la confiabilidad, factores como la velocidad promedio de la transmisión de la información y el procesamiento prioritario de paquetes altamente sensibles a los retardos de tráfico (como el tráfico de voz) se han convertido en aspectos de significativa importancia. Estos cambios se reflejaron en nuevas tecnologías WAN como *Frame Relay* y el Modo de Transferencia Asíncrona (ATM). En dichas redes, se supone que los errores de bits se presentan tan rara vez que es mucho más conveniente sólo descartar los paquetes erróneos. Todos los problemas relacionados con la pérdida de paquetes se asignan a módulos de software específicos de nivel elevado, los cuales no están integrados directamente a las redes *Frame Relay* y ATM.

El predominio del protocolo Internet (IP) ha contribuido a la convergencia de las LAN y WAN. En la actualidad, este protocolo se utiliza sobre cualquier tecnología LAN o WAN, incluidos Internet, *Token Ring*, ATM y *Frame Relay*, con el fin de crear una interred[2] unificada basada en diferentes subredes.

---

[2] La conectividad de redes es un término técnico de uso común que se refiere a una colección de redes interconectadas mediante ruteadores y otros dispositivos. En general, una interred trabaja como una sola red y con frecuencia recibe el nombre de Internet; sin embargo, no debe confundirse con la Internet, la interred más grande que existe y que conecta decenas de miles de redes a nivel mundial.

A partir de la década de 1990, las WAN que trabajaban con base en canales digitales rápidos han ampliado significativamente el rango de servicios desarrollados en las LAN. Fue posible crear servicios cuya operación estuviera relacionada con la entrega de grandes cantidades de información multimedia en tiempo real, incluidos imágenes, video y voz. La Telaraña Mundial de la Información (WWW), un servicio de información en hipertexto que se convirtió en el principal servicio de información en Internet, es el ejemplo más espectacular. Las capacidades interactivas de este servicio excedieron hace mucho tiempo las de servicios similares proporcionadas por las LAN. Por tanto, los arquitectos de las LAN simplemente han tomado este servicio de las WAN. El proceso de transferir tecnologías de Internet en las LAN se convirtió en algo tan popular que muy pronto apareció el término especializado **intranet**.

En la actualidad, en las LAN, los usuarios tienen que poner la misma atención a los mecanismos para proteger la información contra accesos no autorizados que la que ponían en las WAN. Esto se debe a que las LAN ya no están aisladas. A menudo, las LAN tienen acceso al "mundo exterior" por medio de enlaces WAN.

Por último, es necesario mencionar que continúan saliendo al mercado nuevas tecnologías. Originalmente se diseñaron para ambos tipos de redes. El espécimen más notable de la nueva generación de tecnologías es ATM,[3] la cual puede servir como base de las LAN y de las WAN debido a que combina de manera eficaz todo tipo de tráfico en una sola red de transmisión. La familia de tecnologías Ethernet, que surgió a partir de las LAN, sirve como otro ejemplo. El reciente estándar Ethernet 10G hace posible la transmisión de datos a 10 Gbps y se diseñó para troncales tanto de WAN como de LAN de gran tamaño.

> Otra evidencia de la convergencia LAN-WAN es la llegada de las **redes de área metropolitana (MAN)**, las cuales están posicionadas en un lugar intermedio entre las LAN y las WAN. Estas redes se diseñaron para ofrecer servicio a grandes ciudades.

Dichas MAN utilizan canales digitales de comunicación y a menudo fibra óptica, y se caracterizan por tener velocidades troncales de 155 Mbps o mayores; además, proporcionan una forma eficaz de interconectar LAN, así como de conectar LAN con WAN. En un principio, estas redes fueron diseñadas solamente para la transmisión de datos. En la actualidad, el rango de sus servicios se ha ampliado; por ejemplo, las MAN soportan conferencias de video y la transmisión integrada de voz y texto. Las MAN modernas se distinguen por la gran variedad de servicios que ofrecen, los cuales permiten a sus clientes conectar equipo de telecomunicaciones de diferentes tipos, incluidos conmutadores privados (PBX).

1.4.2 Convergencia de las redes de computadoras y de telecomunicaciones

La tendencia hacia la convergencia de diferentes redes de computadoras y de telecomunicaciones de varios tipos ha crecido con el paso de los años. Se intenta crear las llamadas **redes multiservicio** universales, las cuales pueden ofrecer servicios a las redes de computadoras y de telecomunicaciones.

---

[3] El modo de transferencia asíncrona es una tecnología de red que, de manera dinámica, asigna el ancho de banda. ATM utiliza paquetes de datos de longitud fija y un canal fijo entre dos puntos con el fin de transferir datos; además, fue diseñado para soportar múltiples servicios, como voz, gráficas, datos y video de alta definición, a la vez que permite que las compañías telefónicas y de TV por cable puedan asignar ancho de banda a sus clientes.

Las redes de telecomunicaciones incluyen redes telefónicas, de radio y de televisión. La característica principal que las hace similares a las redes de computadoras es que la información es el principal recurso proporcionado por los clientes; sin embargo, estas redes, como regla general, proporcionan información de manera muy diferente. Por ejemplo, las redes de computadoras se diseñaron al inicio para transmitir información alfanumérica, conocida simplemente como datos. Como resultado, las redes de computadora tienen otro nombre: **redes de datos**. Las redes telefónicas y de radio se diseñaron para transmitir información de voz solamente; las redes de televisión pueden transmitir tanto voz como video.

A pesar de ello, la convergencia de las redes de computadoras y telecomunicaciones está progresando.

Primero, es importante notar la *convergencia de tipos de servicio* proporcionada a los clientes. El primer intento de creación de una red multiservicios capaz de ofrecer varios servicios, incluidas telefonía y transmisión de datos, ha dado como consecuencia el desarrollo de la tecnología de la red digital de servicios integrados (ISDN, por sus siglas en inglés). Sin embargo, en la práctica, ISDN proporciona en la actualidad servicios de telefonía principalmente.

Por el momento, Internet es el candidato principal para desempeñar el papel de una red global multiservicios de nueva generación. De especial interés son los nuevos tipos de servicios integrados que combinan varias clases de servicios tradicionales, como la Mensajería Unificada, que combina el correo electrónico, telefonía, fax y mensajería. En la práctica, la telefonía IP, la cual utilizan en la actualidad, directa o indirectamente, millones de usuarios a nivel mundial, ha probado ser la más exitosa; sin embargo, Internet tiene aún un largo camino por recorrer antes de que pueda considerarse una red de nueva generación.

La *convergencia tecnológica* de las redes actuales está basada en la transmisión digital de varios tipos de información, conmutación de paquetes y programación de servicios. La telefonía, hace mucho tiempo, dio varios pasos hacia su integración con las redes de computadoras. Esto se logró debido a la representación de la voz en formato digital, lo cual permitió transmitir tráfico telefónico y de computadora utilizando los mismos canales digitales. En la actualidad, la televisión también es capaz de transmitir información en formato digital. De forma rutinaria, las redes telefónicas emplean una combinación de conmutación de circuitos y de paquetes; por tanto, para transmitir mensajes de servicio (conocidos como mensajes de señal), se usan métodos de conmutación de paquetes, los cuales son similares a los protocolos que se emplean en las redes de computadoras; para la transmisión de voz se utiliza la conmutación de circuitos tradicional.

Los servicios complementarios ofrecidos por las redes telefónicas, como la transferencia de llamadas, la conferencia y las encuestas remotas, podrán asegurarse si se utiliza la **red inteligente (IN)**, la cual representa una red de computadoras con servidores en la que está programada la lógica del servicio.

En la actualidad, los métodos de conmutación de paquetes, están ganando terreno de manera gradual sobre los métodos de conmutación de circuitos, los cuales tradicionalmente se utilizan en las redes telefónicas, aun en el campo de la transmisión de voz. Esta tendencia tiene una razón evidente: la conmutación de paquetes permite un uso más eficaz del ancho de banda de los canales de comunicación y del equipo de conmutación. Por ejemplo, las pausas en una conversación telefónica pueden consumir hasta 40% del tiempo total de la conexión; sin embargo, solamente la conmutación de paquetes posee la habilidad de "cortar" las pausas y utilizar el ancho de banda del canal liberado para transmitir el tráfico de otros usuarios telefónicos. La popularidad de Internet, la cual se basa en la conmutación de paquetes, representa otro argumento a favor de la migración hacia la conmutación de paquetes.

El uso de la conmutación de paquetes para la transmisión simultánea de tráfico heterogéneo (incluidos voz, video y texto) ha acrecentado la importancia de diseñar nuevos métodos para asegurar la **calidad del servicio (QoS)**. Los métodos para asegurar el QoS están diseñados con el fin de minimizar el grado de retardo del tráfico en tiempo real, como el de voz, y para asegurar una velocidad promedio de información y un tráfico dinámico de datos.

Sin embargo, no debe suponerse que los métodos de conmutación de circuitos se han convertido en obsoletos y, por tanto, no tienen futuro; pero, en esta nueva etapa de desarrollo tecnológico, también tiene su aplicación en tecnologías más recientes.

Las redes de computadoras, a su vez, han tomado mucho de las redes telefónicas y de TV. En particular, a pesar de que Internet y las redes corporativas carecen del alto grado de confiabilidad típico de las redes telefónicas, las redes de computadoras han comenzado a integrar a su armadura las herramientas de confiabilidad normalmente utilizadas en las redes telefónicas.

Cada vez resulta más evidente que las redes multiservicio de nueva generación no puedan generarse como resultado de la victoria de una sola tecnología o método. Solamente pueden construirse como resultado de un proceso de convergencia, el cual toma las mejores facilidades y características de cada tecnología y las une de alguna forma que proporcione la calidad que se requiere para soportar los servicios existentes y para crear nuevos. Con el fin de darle nombre a esta tecnología, se ideó el término **redes de infocomunicación** que especifica de manera explícita dos componentes de las redes modernas: informacional (basados en computadoras) y telecomunicaciones. Como este nuevo término no ha obtenido suficiente popularidad todavía, utilizaremos el más estándar y generalmente aceptado —red de telecomunicaciones— en su significado amplio, es decir, incluidas las redes de computadoras.

RESUMEN

- Las redes de computadoras no sólo son el resultado lógico de la evolución de las tecnologías de la computación y de las telecomunicaciones, también representan un caso particular de sistemas de cómputo distribuido y pueden considerarse un medio para transmitir información a través de distancias considerables. Para este último propósito, las redes de computadoras implementan métodos de codificación y multiplexaje de datos desarrollados y adoptados en varios sistemas de comunicación.
- Todas las redes pueden clasificarse, con base en su cobertura geográfica, en las categorías siguientes: redes de área amplia (WAN), redes de área local (LAN) y redes de área metropolitana (MAN).
- Desde el punto de vista cronológico, las WAN fueron las primeras redes en aparecer, éstas conectaban computadoras distribuidas a cientos de kilómetros y a menudo se basaban en enlaces de comunicaciones existentes de baja calidad, lo que dio como resultado bajas velocidades de transmisión de datos. Comparadas con las LAN, las WAN proporcionan un limitado conjunto de servicios, particularmente la transferencia de archivos y el correo electrónico, tras bambalinas en lugar de en tiempo real.
- Generalmente, las LAN abarcan regiones dentro de un radio no mayor que 2.4 kilómetros, y se basan en enlaces caros y de alta calidad que facilitan usar sencillos métodos de transmisión de datos a velocidades de transferencia de datos más elevadas (alrededor de 100 Mbps) que las que permiten las WAN. En general, las LAN proporcionan una gama de servicios implementados en línea.

- Las MAN se diseñaron para dar servicio en ciudades grandes y se caracterizan por tener una distancia considerable entre los nodos de la red (a menudo decenas de kilómetros), proporcionar enlaces de comunicación de alta calidad y soportar altas velocidades de transmisión de datos. Las MAN aseguran una conexión económica y segura entre las LAN y ofrecen a estas últimas el acceso a las WAN.
- La etapa más importante en la evolución de las redes de computadoras fue la llegada de las tecnologías estándar para la conectividad de redes. Entre éstas se incluyen Ethernet, FDDI y *Token Ring*. Dichas tecnologías hacen que diferentes tipos de computadoras se puedan conectar de manera rápida y eficaz.
- A finales de la década de 1980, tanto las LAN como las WAN se caracterizaron por tener diferencias significativas entre su cobertura y calidad de los enlaces de telecomunicaciones, la complejidad de los métodos de transmisión de datos, las velocidades de intercambio de información, el rango de los servicios que proporcionaban y su escalabilidad. Posteriormente, como resultado de la integración de las LAN, WAN y MAN, se llevó a cabo la convergencia de estas tecnologías.
- La tendencia hacia la convergencia de los diferentes tipos de redes es característica no solamente de las LAN y WAN, sino también de otros tipos de redes de telecomunicaciones, incluidas las redes telefónicas, de radio y de TV. Por ahora, la investigación está centrada en la creación de redes multiservicio universal capaces de transmitir, de manera eficaz, información de cualquier tipo, incluidos datos, voz y video.

PREGUNTAS DE REPASO

1. ¿Cuáles características de un sistema multiterminal lo hacen diferente de una red de computadoras?
2. ¿Cuándo se obtuvieron los primeros logros importantes en el campo de la conexión de computadoras, utilizando enlaces de larga distancia?
3. ¿Qué es ARPANET?
   a) Una red de supercomputadoras que pertenece a organizaciones militares e institutos de investigación en Estados Unidos.
   b) Una red internacional de investigación científica.
   c) ¿La tecnología para crear WAN?
4. ¿Cuándo apareció el primer sistema operativo de red?
5. ¿En qué orden se llevaron a cabo los acontecimientos que se listan a continuación?
   a) La invención de la Web.
   b) El desarrollo de tecnologías estándares de LAN.
   c) El comienzo de la transmisión de voz en forma digital a través de redes telefónicas.
6. ¿Cuáles acontecimientos fomentaron el desarrollo de las LAN?
7. ¿Cuándo se estandarizaron las tecnologías siguientes: Ethernet, *Token Ring* y FDDI.
8. Haga una lista con las principales tendencias que tomó la convergencia de las redes de computadoras y de telecomunicaciones.
9. Explique el significado de los términos siguientes: red de multiservicios, red de infocomunicación y red inteligente.

PROBLEMAS

1. Explique por qué las WAN aparecieron antes que las LAN.
2. Mediante el uso de diferentes recursos en Internet, encuentre la relación histórica entre la tecnología X.25 y la red ARPANET.
3. ¿Cree usted que la historia de las redes de computadoras pueda interpretarse como la historia de la evolución de Internet? Fundamente su opinión.

2 PRINCIPIOS GENERALES DEL DISEÑO DE REDES

DESCRIPCIÓN DEL CAPÍTULO

2.1 INTRODUCCIÓN

Cuando usted comienza a estudiar las tecnologías LAN, WAN o MAN como Ethernet, IP o ATM, en seguida se da cuenta de que tienen mucho en común; sin embargo, estas aplicaciones no son idénticas. Por el contrario, cada tecnología o protocolo tiene sus propias características y evita que los usuarios amplíen mecánicamente su conocimiento de un área tecnológica a otra. El mejor método para depurar la eficacia del proceso de aprendizaje es comenzar con una investigación de los principios generales del diseño de redes. Dichos principios constituyen la base que determina la selección de la topología de red, así como los métodos utilizados para enrutar, conmutar y multiplexar flujos de información. Por tanto, un principio muy conocido que establece que "el conocimiento de algunos principios básicos evita que el alumno tenga que memorizar un gran número de hechos" no debe interpretarse de forma literal. Los expertos calificados deben conocer múltiples detalles; sin embargo, comprender objetivamente los principios básicos representa una gran ayuda. Al entender los hechos y detalles individuales y relacionarlos entre sí, los expertos podrán formar un sistema armonioso.

El sistema de principios para construir las redes de datos constituye las soluciones a varios problemas clave, la mayoría de los cuales se encuentran con mucha frecuencia en las redes de telecomunicaciones de todo tipo.

La conmutación es uno de los problemas fundamentales que usted tendrá que enfrentar cuando construya una red. Cada nodo de red involucrado en la transmisión de tráfico debe conmutar dicho tráfico (es decir, habrá que asegurar la comunicación entre los usuarios de la red).

El principio para seleccionar la ruta destinada a transmitir flujos de información mediante la red ejerce una influencia directa en la tecnología de conmutación. La **ruta** (es decir, la secuencia de nodos de red a través de los cuales circulan los datos con el fin de entregarse al nodo de destino) debe seleccionarse de tal modo que se logren dos objetivos de forma simultánea. Primero, los datos de cada usuario deben transmitirse tan rápido como sea posible, con un mínimo retardo en la ruta. Segundo, los recursos de la red deben utilizarse con una máxima eficiencia para asegurar que la red transmite la máxima cantidad de datos de todos los usuarios de la red en todo momento. El problema principal consiste en lograr la combinación de estos objetivos (el objetivo egocéntrico de un usuario individual y el objetivo colectivo de toda la red como un sistema unificado). En forma tradicional, las redes de computadoras resolvieron este problema de manera ineficaz al dar prioridad a los flujos de datos individuales; sólo hasta hace poco tiempo comenzaron a emplear métodos de enrutamiento más avanzados.

En este capítulo estudiamos los principios del multiplexaje de flujos de información y el compartimiento de un medio de transmisión, los problemas del direccionamiento y la selección de la topología de la red, así como las estructuras física y lógica.

2.2 PROBLEMAS DE COMPARTIR RECURSOS DE CÓMPUTO

PALABRAS CLAVE: interfases físicas y lógicas, puerto, tarjetas de interfase de red, controlador, manejador, dispositivos periféricos, impresora, mensajes, cliente, servidor, redirector, sistema operativo, programa distribuido, servicios de red, aplicaciones, aplicaciones de red y sincronización.

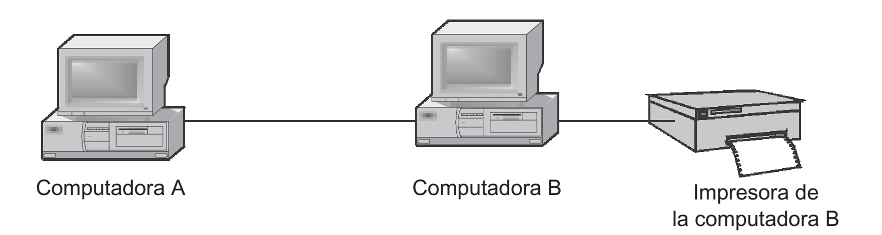


FIGURA 2.1 Compartimiento de la impresora.

La posibilidad de acceder y utilizar dispositivos periféricos (discos, impresoras, graficadores, etc.) conectados a otras computadoras es una de las ventajas más evidentes de las computadoras que están en red. De manera similar a las computadoras independientes, las conectadas en red pueden administrar de modo directo sólo aquellos dispositivos que se encuentran conectados físicamente a ellos. Para permitir que los usuarios de diferentes computadoras puedan compartir dispositivos periféricos, es necesario dotar a la red de algunas herramientas adicionales. Considere estas herramientas en el caso de la red más sencilla que está formada sólo por dos computadoras (figura 2.1). Para comenzar, considere la interacción entre una computadora y un dispositivo periférico.

2.2.1 Interacción entre computadoras y dispositivos periféricos

Para organizar la interacción entre una computadora y un dispositivo periférico, ambos cuentan con interfases físicas externas.

En un sentido amplio, la interfase representa una lógica o física definida formalmente entre los objetos por comunicarse, los cuales son independientes entre sí. La interfase define parámetros, procedimientos y características de la interacción entre objetos.

La **interfase física** (también llamada **puerto**) se define por un conjunto de conexiones eléctricas y características de las señales. Como una regla, representa un conector con un conjunto de contactos, cada uno de los cuales tiene un propósito específico. Debe contar con un grupo de contactos para la transmisión de datos, un contacto para la sincronización de éstos, y así sucesivamente. El par de enchufes se encuentra conectado mediante un cable diseñado a partir de un conjunto de alambres que conectan los contactos respectivos (figura 2.2).

La **interfase lógica** es un conjunto de mensajes de información con un formato predefinido que utilizan dos dispositivos (en este caso, una computadora y un dispositivo periférico) o programas para intercambiar datos entre sí, además de un conjunto de reglas que determinan la lógica de este intercambio.

La interfase paralela Centronics (transmisión de datos en bytes), la cual, como regla general, está diseñada para conectar impresoras, y la interfase (también conocida como puerto COM) serie RS-232C (transmisión de datos en bits) son ejemplos ilustrativos de interfases estándar que se utilizan en las computadoras. La última interfase se usa más universalmente, pues, además de las impresoras, existen numerosos dispositivos que la soportan, incluidos graficadoras y ratones. También hay interfases especializadas que se diseñaron con el fin de conectar periféricos muy particulares como equipos especiales para realizar experimentos físicos.

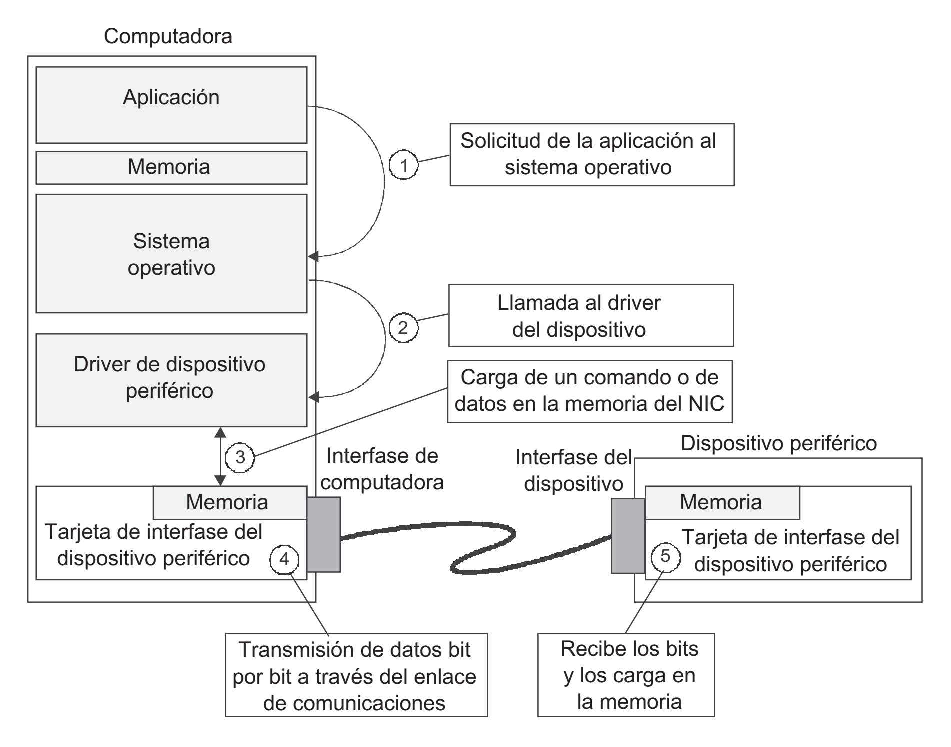


FIGURA 2.2 Conexión entre una computadora y un dispositivo periférico.

> Las operaciones de interfase en las computadoras están implantadas mediante una combinación de hardware y software. La tarjeta de interfase (un dispositivo de hardware también conocido como controlador o adaptador) y algunos programas especiales administran los dispositivos físicos. A menudo, dicho software se llama *controlador de dispositivos periféricos*.

En los dispositivos periféricos, dicha interfase, muy a menudo, está implementada como un dispositivo hardware–**controlador**,[1] a pesar de que también se pueden encontrar controladores administrados por software, los cuales están equipados con un procesador interno. Éste es el caso de los periféricos cuya lógica de operación es sofisticada. Las impresoras modernas representan buenos ejemplos de este tipo de controladores.

Los dispositivos periféricos pueden aceptar de la computadora tanto datos (por ejemplo, información que deba ser impresa) como instrucciones, en respuesta a cuál controlador de dispositivo periférico ha de llevar a cabo las acciones específicas. Por ejemplo, el controlador de impresora puede soportar un conjunto de comandos simples, como *Print Character*, *Line Feed*, *Carriage Return* y *Eject paper from the printer,* los cuales recibe de una computadora por medio de la interfase y termina administrando los componentes electromecánicos de la impresora.

Como regla general, el intercambio de datos por medio de la interfase es bidireccional; por ejemplo, aun las impresoras que por su naturaleza representan dispositivos de salida, envían

[1] Los términos *tarjeta de interfase*, *adaptador* y *controlador* se usan a veces como sinónimos; sin embargo, para distinguir al controlador instalado dentro de la computadora del controlador que está dentro de la impresora, utilizaremos el término *tarjeta de interfase* para el primero, mientras el de controlador para el segundo.

información acerca de su estatus a la computadora. Considérese la secuencia de operaciones que utiliza la aplicación para enviar datos a la impresora.

- Una aplicación que necesite enviar sus datos a una impresora, solicita al sistema operativo que lleve a cabo una operación de entrada-salida. Para procesar esta solicitud se deben especificar los datos siguientes: dirección en la RAM de los datos, el identificador del dispositivo periférico que se requiera y la operación que se deba realizar.
- Una vez recibida dicha solicitud, el sistema operativo llama al controlador de impresión que especifica la aplicación solicitada. Las demás acciones que se requieran para efectuar la operación de entrada-salida de la computadora se encuentran implementadas en la tarjeta de interfase que está bajo las órdenes del controlador.
- En cuanto al controlador de impresión, éste trabaja con los comandos que maneja el controlador de impresión: *Print Character*, *Line Feed*, *Carriage Return* y *Eject paper from printer.* El controlador forma la secuencia de códigos de comando y los coloca en la memoria de la tarjeta de interfase, la cual posteriormente las transfiere byte por byte al controlador de impresión. Es factible desarrollar diferentes controladores para el mismo dispositivo controlador, siempre y cuando se utilice el mismo conjunto de comandos, aunque trabajen con algoritmos distintos para administrar los dispositivos periféricos.
- Para efectos de una operación coordinada del controlador y el adaptador de interfase, este último lleva a cabo operaciones de bajo nivel que le permiten interpretar los datos y comandos que le transmite el controlador como un flujo uniforme de bytes, sin que éste requiera comprender su significado. Después de recibir el siguiente byte del controlador, el adaptador de interfase comienza a transmitir bits de manera secuencial hacia el cable de la interfase, representando cada bit mediante una señal eléctrica. Para informar al controlador del dispositivo periférico que la transmisión del siguiente byte está a punto de comenzar, la tarjeta de interfase genera una señal de arranque específica antes de transmitir el primer bit de información. Después de transmitir el último bit de información, la tarjeta de interfase genera la señal de paro. Estas señales de arranque y paro se utilizan para sincronizar la transmisión de bytes. Una vez que el controlador reconoce el bit de arranque, éste comienza a recibir bits de información y forma un byte en su memoria de recepción.
- Además de los bits de información, el adaptador transmite el bit de control de paridad con el fin de asegurar la confiabilidad del intercambio de datos. Siempre y cuando los datos sean transmitidos de manera correcta, el controlador interpreta el byte recibido y empieza a llevar a cabo la operación de impresión que se solicitó.
- Una vez que ha terminado de imprimir todos los caracteres del documento, el controlador de impresión informa al sistema operativo que ha finalizado la solicitud. El sistema operativo, a su vez, informa a la aplicación acerca de este evento.

2.2.2 Interacción más simple entre dos computadoras

Reconsideremos el problema inicial: ¿cómo puede un usuario que trabaja con alguna aplicación que corre en la computadora A imprimir texto en una impresora conectada en la computadora B (figura 2.3)?

Las aplicaciones que corren en la computadora A no pueden acceder directamente a los recursos de la B, como discos, archivos o impresoras. Para acceder a estos recursos, la aplicación solamente debe llamar a otro programa que corra en la computadora cuyos recursos necesite utilizar. Dichas solicitudes están implantadas en forma de **mensajes** transmitidos

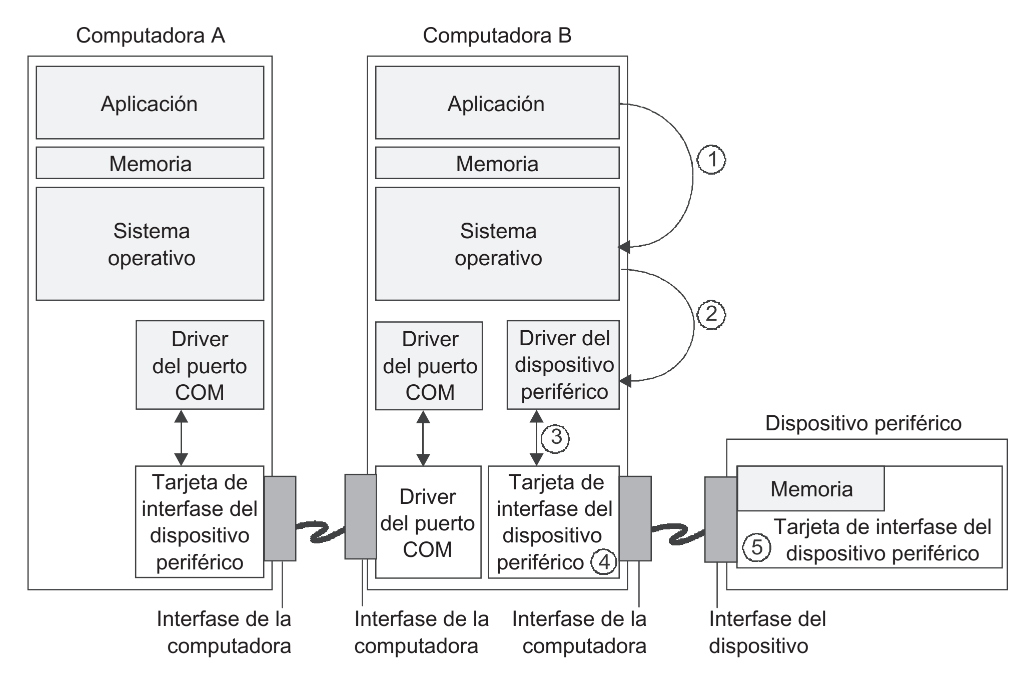


FIGURA 2.3 Compartimiento de la impresora.

por medio de enlaces de comunicaciones que conectan a las computadoras participantes en la red. En general, dichos mensajes contienen tanto instrucciones (por ejemplo, abrir un archivo) como información que será procesada (por ejemplo, el contenido de un archivo específico).

Los mecanismos de interacción que se utilizan en la comunicación entre las computadoras conectadas a una red han tomado muchas ideas del método de interacción que se usa en la comunicación entre una computadora y sus periféricos. En su forma más simple, la comunicación entre computadoras se llevará a cabo si se emplean las herramientas que organizan la interacción entre una computadora y sus dispositivos periféricos. Por ejemplo, para lograr lo anterior puede utilizarse la interfase serial: el puerto COM. Los puertos COM en *ambos lados* trabajan con sus controladores. Trabajando en conjunto, ambos aseguran la transmisión de un byte de información a través del cable que conecta las dos computadoras.

NOTA *En las LAN prácticas, dichas funciones son llevadas a cabo por las tarjetas de interfase de red (NIC, por sus siglas en inglés), a menudo llamadas adaptadores de red, y por sus controladores. Desde el punto de vista de la computadora, el adaptador de red es un dispositivo periférico como cualquier otro, el cual no es diferente del controlador de la impresora.*

Por tanto, se ha definido el mecanismo de intercambio de bytes entre dos computadoras; sin embargo, esta simple herramienta no es suficiente para resolver el problema de imprimir texto en una impresora conectada en otra computadora. Es necesario asegurar que la computadora B sepa qué operación tiene que llevar a cabo con los datos que se le transmitieron, en cuál de los dispositivos disponibles debe imprimir, cómo ha de aparecer el texto que se va a imprimir, etc. Las aplicaciones A y B deben establecer todas estas condiciones mediante el intercambio de mensajes.

Asimismo, las aplicaciones deben saber cómo interpretar la información que reciban una de la otra. Con este fin en mente, los diseñadores de las aplicaciones A y B deben convenir no sólo en el formato y la semántica del mensaje, sino también en que la ejecución de cualquier operación de impresión remota debe comenzar con la transmisión de un mensaje, preguntando si la aplicación B está lista, en que el siguiente mensaje deba contener identificadores de la computadora y el usuario que ha realizado la solicitud, en que un código específico sirva para señalar una terminación anormal, etc. Como se observará más adelante, estas reglas definen el protocolo de interacción entre las aplicaciones.

Considere las interacciones entre todos los elementos de esta pequeña red, la cual hará factible que una aplicación que corra en la computadora A imprima un documento en la impresora conectada a la computadora B.

- La aplicación A debe generar un mensaje para la aplicación B, solicitándole que imprima un texto. Este mensaje se envía a una memoria RAM. Para transmitir esta solicitud hacia la computadora remota B, la aplicación A llama al sistema operativo local (SO); a su vez, el SO local llama al controlador del puerto COM y lo transfiere a la dirección de la memoria RAM, donde se puede encontrar el mensaje que se solicitó. De acuerdo con el método que se acaba de describir, el controlador del puerto COM y el controlador de la computadora A interactúan con el controlador del puerto COM y el controlador de la computadora B, con el fin de enviar el mensaje, byte por byte, a la computadora B.
- El controlador del puerto COM de la computadora B espera que llegue información entrante proveniente del exterior. En algunos casos, se llama al controlador de manera asíncrona mediante interrupciones provenientes del controlador ojo. Se crea una confusión al traducir driver y controller. Una vez que se ha recibido el siguiente byte y verificado que esté correcto, el controlador lo almacena en la memoria de la aplicación B.
- La aplicación B recibe el mensaje, lo interpreta y, en función de su contenido, genera la solicitud al sistema operativo local para llevar a cabo las acciones específicas con la impresora. El sistema operativo de la computadora B envía esta solicitud al driver de la impresora.
- Durante el proceso de impresión pueden surgir situaciones que requieran ser reportadas a la aplicación A. En este caso, se utiliza un diseño simétrico. La solicitud de transmisión del mensaje viaja de la aplicación B al SO local que corre en la computadora B. Los controladores del puerto COM y los de ambas computadoras organizan la transmisión del mensaje byte por byte, el cual se carga posteriormente en la memoria de la aplicación A.

Los usuarios de muchas otras aplicaciones (editores de texto o de gráficas, sistemas de administración de bases de datos, etc.) pueden acceder a archivos remotos. Evidentemente, no es razonable diseñar las funciones de la aplicación A descritas, en todas las aplicaciones estándar que deban utilizarse en un ambiente de red, aunque algunas aplicaciones cuentan con funciones de red incorporadas. En general, dichas aplicaciones tienen requerimientos muy estrictos en cuanto a la velocidad del intercambio de datos; sin embargo, la solución más eficaz es el desarrollo de módulos de software especializado designados exclusivamente para generar las solicitudes a las máquinas remotas y para recibir los resultados destinados a todas las aplicaciones. Dichos módulos de software se conocen por lo general como clientes y servidores.

Cliente es el módulo diseñado para integrar mensajes de solicitud a una máquina remota desde diferentes aplicaciones, recibir los resultados y transferirlos a las aplicaciones correspondientes.

Servidor es el módulo que debe *escuchar*, de forma permanente, las solicitudes de clientes que provienen de la red y que estén dirigidas hacia dispositivos específicos conectados a esa computadora. Una vez que el servidor recibe la solicitud del cliente, éste trata de procesarla y realizarla, a veces con ayuda del SO local. Un servidor puede atender las solicitudes de varios clientes de manera secuencial o en paralelo.

La característica más conveniente y útil de un componente cliente es la capacidad para distinguir entre las solicitudes a recursos locales y a recursos remotos. Si un programa cliente puede hacer lo anterior, no importará si las aplicaciones tienen que ver con recursos locales o remotos, pues el programa cliente reconoce las solicitudes remotas y las *retransmite* a la máquina remota. De aquí que el módulo cliente de una aplicación de red también se conoce con el nombre de *redirector*. A veces, las funciones responsables de reconocer solicitudes locales y remotas están implantadas en un módulo de software independiente; en este caso, sólo este módulo, mas no todo el componente cliente, se llama *redirector*.

El software cliente-servidor lleva a cabo funciones del sistema relacionadas con brindar servicio a las solicitudes de todas las aplicaciones que corren en la computadora A para acceder remotamente a los recursos de la computadora B (impresora, archivos, fax, etc.). Para que las aplicaciones que corren en la computadora B puedan acceder a los recursos de la computadora A, este diseño debe complementarse simétricamente por medio del software cliente para la computadora B y un módulo servidor para la computadora A.

La figura 2.4 muestra el método de interacción cliente y servidor con las aplicaciones y el sistema operativo local. A pesar de que hemos considerado el método más simple de interacción entre dos computadoras, las funciones del programa que aseguran el acceso a una impresora remota tienen mucho en común con un sistema operativo que corre en una red formada por un gran número de computadoras conectadas de manera más sofisticadas.

NOTA *Los términos cliente y servidor se utilizan para designar tanto módulos de software como computadoras como un todo. Si una computadora brinda sus recursos a otras computadoras conectadas a la red, dicha computadora se conoce con el nombre de servidor. Una computadora que utiliza los recursos provistos por un servidor se conoce como cliente. A menudo la misma computadora puede llevar a cabo ambas funciones de manera simultánea.*

2.2.3 Aplicaciones de red

Brindar a los usuarios el acceso compartido a determinados tipos de recursos (por ejemplo, a archivos) equivale a brindar el servicio (servicio de archivos, en este caso). En general, el sistema operativo de red soporta varios tipos de servicio de red para sus usuarios: servicio de archivos, servicio de impresión, servicio de correo electrónico, servicio de acceso remoto (RAS), etc. Los programas que incluyen servicios de red se clasifican como programas distribuidos.

Un *programa distribuido* está formado por diversos componentes que interactúan (en el ejemplo de la figura 2.5 se muestran dos de dichos módulos de software). Como regla general, cada componente puede correr en computadoras de red distintas, que es lo más usual.

Los servicios de red son programas de *sistema* distribuidos que con mucha frecuencia forman una parte integral del sistema operativo.

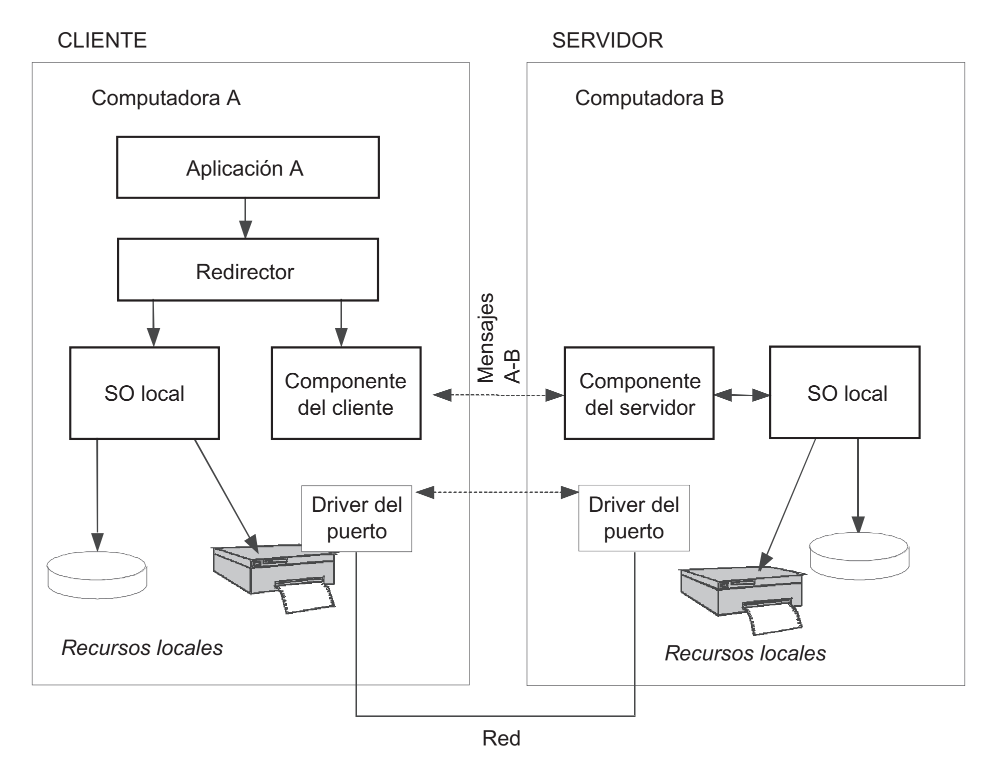


FIGURA 2.4 Interacción de los diversos componentes de software cuando se conectan dos computadoras.

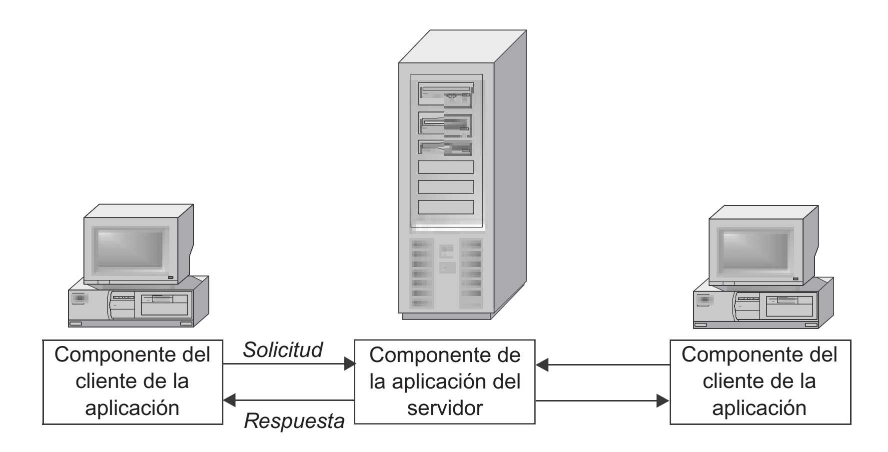


FIGURA 2.5 Interacción de los módulos de una aplicación distribuida.

Sin embargo, existen también programas de usuario distribuidos: **aplicaciones**. Una aplicación **distribuida** también incluye varios componentes, cada uno de los cuales lleva a cabo ciertas operaciones con el fin de realizar determinadas tareas del usuario. Por ejemplo, una parte de dicha aplicación que corre en una estación de trabajo del usuario final puede soportar una interfase gráfica de usuario (GUI). Otro módulo puede correr en una

computadora dedicada de gran capacidad y llevar a cabo el procesamiento estadístico de los datos proporcionados por el usuario; la tercera parte podría cargar los resultados en la base de datos que reside en una computadora donde está instalado el sistema estándar de administración de bases de datos (DBMS). Las aplicaciones distribuidas emplean totalmente el potencial del procesamiento distribuido que proporcionan las redes de datos. Por tanto, a menudo se llaman **aplicaciones de red.**

NOTA *Es necesario señalar que no toda aplicación que corra en un ambiente de red puede clasificarse como una "aplicación real de red". Existe una amplia gama de aplicaciones muy populares que, a pesar de que pueden correr en un ambiente de red, no representan programas distribuidos, ya que sus componentes no pueden estar distribuidos en diversas computadoras. Sin embargo, aun dichas aplicaciones pueden gozar de los beneficios que proporcionan las redes, gracias a la presencia de los servicios de red incorporados en el sistema operativo. Una parte significativa de la historia de las LAN está dirigida al uso de dichas aplicaciones. Considere cómo trabajaban los usuarios con el DBMS de dBase, el cual era muy popular en esa época. En realidad, dBase era uno de los primeros DBMS para las PC. En general, los archivos de bases de datos accesados por todos los usuarios de la red residen en el servidor de archivos. El DBMS se instaló en cada computadora cliente como un módulo de software independiente. En un inicio, dBase fue diseñado para procesar datos locales solamente (es decir, los datos que residen en la misma computadora en la que reside el DBMS). Los usuarios arrancaban dBase en la computadora local y el programa buscaba los datos en discos duros locales sin tener en cuenta la existencia de una red de computadoras. Para procesar datos remotos utilizando dBase, el usuario tenía que acceder a servicios de archivos, los cuales transferían datos del servidor a la computadora cliente y daba la impresión al DBMS de que estos datos eran almacenados en forma local.*

La mayoría de las aplicaciones utilizadas en las LAN a mediados de la década de 1980 no eran distribuidas en realidad. Esto es comprensible, ya que en un inicio estos programas se escribieron para computadoras independientes. A medida que las computadoras fueron más populares, dichas aplicaciones se instalaron en el ambiente de red. Aunque el desarrollo de aplicaciones distribuidas prometía proporcionar un gran número de ventajas (como una reducción del tráfico de red y una especialización de acuerdo con las funciones de las computadoras), en la práctica mostró ser una tarea difícil de llevar a cabo. Fue necesario resolver muchos problemas adicionales. Los diseñadores tuvieron que decidir cuántos módulos debía contener la aplicación, cómo debían interactuar éstos con el fin de asegurar que después de fallas o problemas de funcionamiento los módulos restantes no resultaran afectados, etc. Hasta la actualidad, sólo una pequeña parte de las aplicaciones existentes son realmente distribuidas; sin embargo, es evidente que el futuro pertenece a estos tipos de aplicaciones, ya que éstas pueden implantar el potencial de las redes en el campo del procesamiento de datos en paralelo.

2.3 PROBLEMAS DE LA TRANSMISIÓN FÍSICA DE DATOS UTILIZANDO ENLACES DE COMUNICACIONES

PALABRAS CLAVE: codificación, métodos por pulsos y potenciales, enlaces de comunicación, sincronización, suma verificadora, reconocimiento, carga ofrecida, tasa de información (rendimiento), capacidad, ancho de banda, enlaces dúplex, half dúplex y enlaces simples.

Aun cuando se consideran las redes más simples que están formadas por dos computadoras, se pueden observar muchos problemas característicos de cualquier red de computadoras. En primera instancia, existen problemas relacionados con la transmisión física de señales utilizando enlaces de comunicación.

2.3.1 Codificación

En el campo de las computadoras, la información se representa mediante el uso del código binario. Dentro de la computadora, las señales eléctricas discretas corresponden a unos y ceros.

> La representación de datos en forma de señales eléctricas u ópticas se conoce como *codificación*.

Existen varios métodos para codificar dígitos binarios. Por ejemplo, cuando se utiliza el famoso método potencial, un nivel específico de voltaje representa un 1 y otro corresponde a un 0. Otro método posible es el del pulso, en el cual se emplean pulsos de diferente polaridad para representar los dígitos binarios.

Se pueden utilizar métodos similares de codificación para la transmisión de datos de una computadora a otra mediante el uso de enlaces de comunicación; sin embargo, estos enlaces de comunicación tienen características diferentes respecto a las que residen dentro de una computadora. La diferencia principal entre los enlaces de comunicación externos y los internos consiste en que los externos son de una longitud significativamente mayor; además, éstos se encuentran fuera de la carcasa protegida de la computadora y se extienden a lo largo de áreas donde, con frecuencia, predominan ambientes con ruido electromagnético intenso. Estos factores provocan distorsiones en los pulsos rectangulares (por ejemplo, distorsiones de los frentes del pulso) que son más significativas que las presentadas dentro de la carcasa de una computadora. Como consecuencia, cuando se tenga que asegurar el reconocimiento de pulsos en el extremo receptor del enlace de comunicaciones, no siempre será posible utilizar las mismas velocidades de transmisión y métodos de codificación dentro y fuera de la computadora. Por ejemplo, debido a la elevada carga capacitiva del enlace de comunicaciones, el frente del pulso se eleva muy lentamente. Por tanto, para evitar el traslapamiento de los frentes delantero y trasero de pulsos adyacentes, así como asegurar que el pulso cuente con el suficiente tiempo para elevarse al nivel requerido, es necesario reducir la velocidad de transmisión.

En las redes de computadoras se utiliza la codificación potencial y por pulsos de los datos discretos, así como la **modulación**: un método específico para representar datos que nunca se emplea dentro de las computadoras (figura 2.6). Cuando se usa la modulación, la información discreta se representa mediante una señal de frecuencia senoidal que se envía en forma confiable a través del enlace de conexión.

La codificación potencial o por pulsos se utiliza en los *enlaces de comunicación de alta calidad*; se prefiere la modulación basada en señales senoidales cuando el enlace introduce distorsiones significativas en las señales que se transmiten. Por ejemplo, la modulación se emplea en las WAN cuando se transmiten datos a través de líneas telefónicas analógicas, las cuales se desarrollaron para la transmisión de voz en forma analógica y, por tanto, no son apropiadas para usarse en la transmisión directa de pulsos.

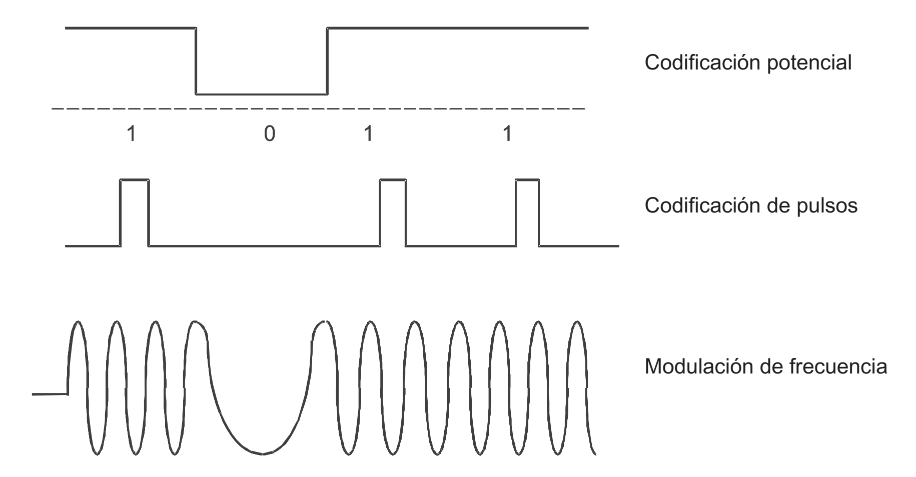


FIGURA 2.6 Ejemplos de algunos métodos para representar información en forma discreta.

El *número de alambres* de los enlaces de comunicación que conectan a las computadoras también influye en el método de transmisión de las señales. Con la finalidad de reducir el costo de los enlaces de comunicación de las redes, una solución común es disminuir el número de alambres. Para ello, por lo regular se emplea la transmisión de datos secuencial bit por bit, la cual requiere un solo par de alambres; el método de transmisión de datos que se utiliza dentro de una computadora transmite todos los bits que forman un byte e incluso varios bytes en paralelo.

La sincronización del transmisor de una computadora y el receptor de otra representa otro problema al que uno se enfrenta cuando se transmiten señales de una computadora a otra. Cuando se organiza la interacción de los módulos de hardware dentro de una computadora, este problema se resuelve de manera sencilla, ya que todos los módulos se encuentran sincronizados mediante el generador de pulsos de reloj común. Los problemas de sincronización que surgen cuando se diseña la comunicación entre computadoras podrán resolverse mediante el intercambio de pulsos especiales de reloj para sincronización si se usan líneas independientes y mediante una sincronización periódica si se emplean códigos predefinidos o pulsos con una forma diferente de la de los pulsos de datos.

Aun después de seleccionar las velocidades apropiadas para el intercambio de datos, el uso de enlaces de comunicación con las características requeridas y el método de sincronización del transmisor y el receptor, persiste cierta probabilidad de que se presente una distorsión en algunos bits de los datos transmitidos. Con el fin de asegurar la confiabilidad en la transmisión de datos entre computadoras, se utiliza por lo general un método estándar: el **cálculo de la suma verificadora** y su transmisión mediante el uso de enlaces de comunicación después de cada byte o bloque de bytes. Con mucha frecuencia, la señal de reconocimiento se encuentra incluida en el protocolo de intercambio de datos como un componente obligatorio. Este **reconocimiento** se envía del emisor al receptor y sirve para confirmar que la recepción de los datos haya sido la correcta.

2.3.2 Características de los enlaces físicos

Existen múltiples características importantes relacionadas con la transmisión del tráfico que se utiliza en los enlaces físicos. Se estudiarán aquí las que usted requiere, mientras que algunas otras se analizarán en el capítulo 6.

- La **carga ofrecida** es el flujo de datos desde el usuario hasta la entrada de la red. La carga ofrecida puede caracterizarse por la velocidad de los datos de entrada a la red. Por lo regular, la velocidad de transmisión se mide en bits, kilobits, megabits y así sucesivamente, por segundo, y se representa como bps, Kbps, Mbps, etcétera.
- La **velocidad (tasa) de información** o rendimiento (ambos términos son sinónimos, por lo cual pueden intercambiarse) es la velocidad real del flujo de datos a través de la red. Puede ser menor que la carga ofrecida ya que la red, como cualquier otro sistema real, puede comportarse de una forma no deseable por el usuario. Por ejemplo, los datos pueden dañarse o perderse y, como resultado, la velocidad real de la información puede disminuir.
- La **capacidad** se define como la velocidad máxima posible de transmisión de datos utilizando un tipo de enlace específico. La parte específica de esta característica consiste en que su valor depende de las características físicas del medio y del método seleccionado para transmitir información discreta utilizando este medio. Por ejemplo, la capacidad del enlace en la red Ethernet por fibra óptica es de 10 Mbps. Este valor especifica la velocidad límite de la combinación de determinado medio de transmisión (fibra óptica, en este caso) y la tecnología seleccionada (Ethernet). Esta velocidad límite depende del método de codificación de datos, de la velocidad de reloj de la señal de información y de otros parámetros. Es factible desarrollar otra tecnología de transmisión de datos para el mismo medio de transmisión, la cual estará caracterizada por otro valor de capacidad. Por ejemplo, la tecnología Fast Ethernet permite transmitir datos utilizando la misma conexión por fibra óptica a una velocidad máxima de 100 Mbps; la tecnología Gigabit Ethernet alcanza una velocidad máxima de transmisión de 1 000 Mbps. El transmisor de determinado dispositivo de comunicaciones debe trabajar a una velocidad igual a la de la capacidad del enlace, la cual a menudo se conoce como *tasa de bits del transmisor*.
- **Ancho de banda.** El uso de este término es algo confuso, debido a que puede tener dos significados diferentes. En primera instancia, puede utilizarse para designar una característica física del medio de transmisión físico. En este caso, el término se refiere al ancho de una banda de frecuencias a la que una línea de comunicaciones transmite sin experimentar distorsiones significativas. El origen de dicho término es evidente a partir de esta definición; por otro lado, el mismo término puede utilizarse como sinónimo de capacidad. En el primer caso, el ancho de banda se mide en Hertz (Hz), mientras que en el segundo se mide en bits por segundo. Los significados de este término se distinguen con base en el contexto, aunque a menudo esto puede ser complejo. Ciertamente, sería mejor si se utilizaran términos diferentes para cada característica; sin embargo, es difícil modificar ciertas tradiciones. Este uso doble del término ancho de banda se ha hecho muy popular y puede encontrarse en múltiples libros y estándares; por tanto, también utilizaremos esta nomenclatura. Además de lo anterior, es necesario tener en cuenta que el segundo significado de este término es muy común y, por ende, se prefiere, excepto cuando se desvía del significado real.

El siguiente grupo de características de un enlace de comunicaciones está relacionado con la posibilidad de transmitir información por medio de este enlace *en una o ambas direcciones.*

En el curso de la interacción entre dos computadoras, generalmente es necesario transmitir información en ambas direcciones, es decir, de la computadora A a la B y viceversa. Aun cuando a los usuarios les parezca que solamente reciben información (descargando archivos de música de Internet) o sólo envían información (enviando un mensaje de correo electrónico), el intercambio de información es bidireccional. Existen dos flujos de datos: el

flujo principal, que es de interés práctico al usuario, y el flujo auxiliar, que se transmite en la dirección opuesta. Este flujo auxiliar de datos está formado por los reconocimientos de recepción del flujo de datos principal.

Los enlaces físicos se clasifican con base en su capacidad para transmitir información en ambas direcciones.

- El **enlace dúplex** asegura la transmisión simultánea de información en ambas direcciones. Los enlaces dúplex pueden abarcar dos medios físicos de transmisión, cada uno de los cuales se utiliza para transmitir información en una sola dirección. También es factible usar el mismo medio para la transmisión simultánea de flujos de datos en ambas direcciones; sin embargo, en este caso, es necesario emplear métodos adicionales para aislar cada flujo.
- Los **enlaces half-dúplex** también aseguran la transmisión de información en ambas direcciones. Esta transmisión no es simultánea, sino por turnos, lo cual significa que durante espacios de tiempo específicos la información se transmite en una dirección y, durante el periodo siguiente, ésta viaja en la dirección contraria.
- El **enlace simplex** permite la transmisión de información en una sola dirección. Con mucha frecuencia, los enlaces dúplex están formados por dos simplex.

Varios aspectos de la transmisión física de datos se estudiarán con mayor profundidad en la parte II de este libro: *Tecnologías de una capa física*.

2.4 PROBLEMAS DE INTERACCIÓN ENTRE ALGUNAS COMPUTADORAS

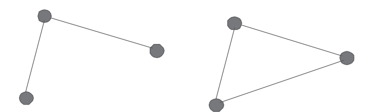
PALABRAS CLAVE: topología, configuración, gráfica, topología totalmente conectada, malla, anillo, estrella, bus común, árbol, estrella jerárquica, topología híbrida, concentrador, direccionamiento, difusión amplia (*broadcast*), difusión dirigida a una instancia (*unicast*), difusión dirigida a cualquier instancia (*anycast*), numérico, simbólico, hardware, espacio de direcciones, espacio de direcciones plano (lineal) o jerárquico, direcciones lógicas, dirección MAC, protocolos de resolución de direcciones, números de puerto, conmutación, enrutamiento.

Hasta el momento, hemos descrito la red más simple, la cual incluye solamente dos máquinas. Cuando un número mayor de computadoras se conectan en red, surgen nuevos problemas.

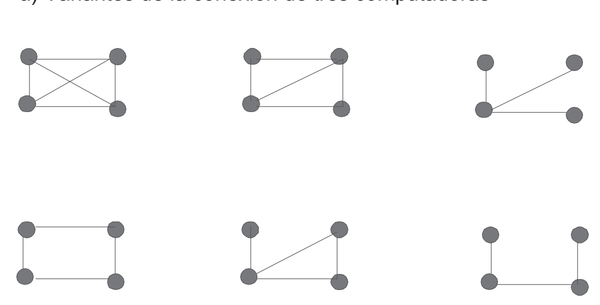
2.4.1 Topología de los enlaces físicos

En cuanto surge el problema de interconectar más de dos computadoras, es necesario decidir cómo interconectarlas. En otras palabras, usted debe seleccionar la configuración de los enlaces físicos, lo cual se conoce con el nombre de *topología*.

La **topología de red** se refiere a la configuración de una gráfica cuyos vértices corresponden a los nodos de red (por ejemplo, computadoras) y al equipo de comunicaciones (por ejemplo, ruteadores), cuyos extremos representan las conexiones físicas o de información entre ellos.



a) Variantes de la conexión de tres computadoras



b) Variantes de la conexión de cuatro computadoras

FIGURA 2.7 Posibles variantes de la conexión de múltiples computadoras en una red de computadoras.

El número de configuraciones posibles se eleva de manera considerable al aumentar el número de dispositivos a conectarse. Por ejemplo, se podrán conectar tres computadoras si se utilizan dos métodos (figura 2.7*a*); en una configuración con cuatro computadoras existen seis configuraciones topológicamente distintas (siempre y cuando las computadoras no puedan distinguirse una de la otra), como se muestra en la figura 2.7*b*.

Cada computadora puede conectarse a cualquier otra o éstas se pueden conectar de manera secuencial. En este último caso, suponga que ambas se comunicarán mediante la transmisión de mensajes "de tránsito". Los **nodos de tránsito**, en este caso, deben estar equipados con herramientas especiales que les permitan llevar a cabo tal operación intermedia. Tanto una computadora universal como un dispositivo especializado pueden funcionar como un nodo de tránsito.

La mayoría de las características de la red dependen de la elección de la topología. Por ejemplo, la disponibilidad de diferentes rutas entre los nodos incrementa la confiabilidad de la red y asegura la posibilidad de balancear la carga de los enlaces de transmisión. La facilidad de conectar nuevos nodos, algo típico de algunas topologías, hace que la red sea extensible. A menudo, las consideraciones económicas dan como resultado una selección de topologías para las que la longitud mínima total de los enlaces de comunicaciones es un aspecto característico.

Entre la gran variedad de posibles configuraciones, es posible distinguir entre topologías total y parcialmente conectadas.

Una **topología totalmente conectada** (figura 2.8*a*) corresponde a una red en la que cada computadora se encuentra conectada directamente a las demás. A pesar de su simplicidad lógica, esta topología es muy voluminosa e ineficaz. Cada computadora debe contar con un número suficiente de puertos de comunicación para conectarse con las demás computadoras. Por cada par de computadoras debe haber un enlace físico de conexión. (Debe haber dos enlaces cuando una sola línea no sea suficiente para la transmisión bidireccional.) Las topologías totalmente conectadas se emplean muy rara vez en redes grandes, pues para conectar N nodos es necesario contar con $N(N-1)/2$ enlaces de conexión dúplex (es decir, el número de enlaces está relacionado con el número de nodos mediante una función cuadrada). Con

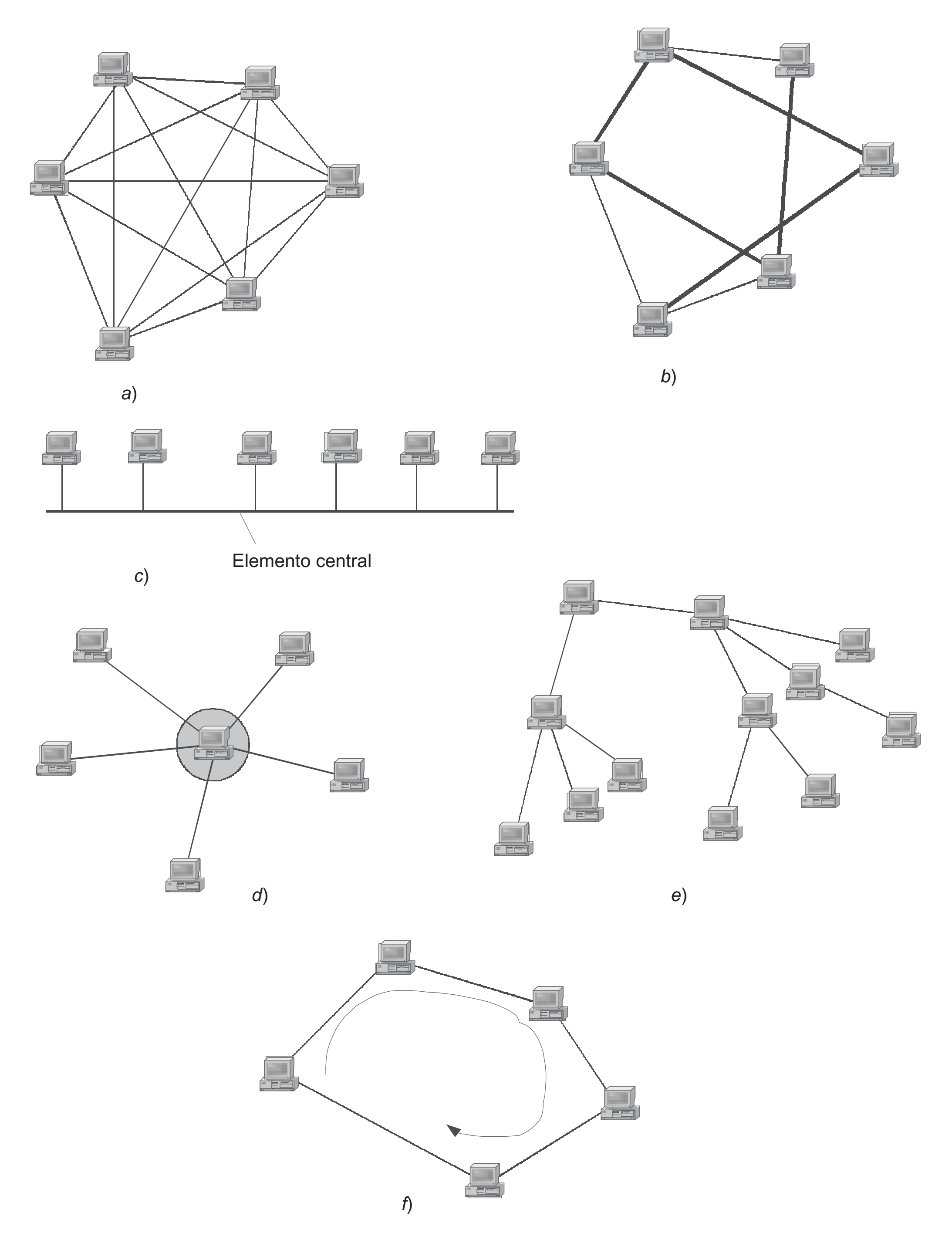


FIGURA 2.8 Topologías típicas de red.

mucha frecuencia, este tipo de topología se utiliza en complejos multimáquina o en pequeñas redes que conectan un número muy limitado de computadoras.

Los demás tipos de red se basan en **topologías parcialmente conectadas**, en las que se puede requerir la transmisión de datos utilizando otros nodos de la red, para llevar a cabo el intercambio de datos entre dos computadoras.

La **topología en malla**[2] se obtiene a partir de la topología totalmente conectada al suprimir algunos de sus enlaces (figura 2.8*b*). Las topologías en malla hacen posible que un gran número de computadoras se puedan conectar y es una característica típica de las redes de gran tamaño.

En las redes con **topología en anillo** (figura 2.8*f*), los datos se transmiten alrededor del anillo de computadora a computadora. La ventaja principal del anillo consiste en su propiedad para proporcionar enlaces redundantes. Cada par de nodos se conecta mediante dos rutas: una en el sentido de las manecillas del reloj y la otra en el sentido opuesto. El anillo representa una configuración muy apropiada para brindar retroalimentación, pues los datos, una vez que han recorrido todo el anillo, regresan a su nodo de origen. Debido a esta característica, el nodo de origen puede controlar el proceso de entrega de los datos al nodo de destino. Con mucha frecuencia, esta propiedad del anillo se utiliza para probar la conectividad de la red y para buscar aquellos nodos que no funcionan de manera correcta. Por otro lado, en las redes con topología de anillo es necesario tomar medidas especiales para asegurarse de que, cuando una computadora falle o deje de operar de forma temporal, no falle el circuito de comunicaciones de los demás nodos de la red.

La **topología en estrella** (figura 2.8*d*) supone que cada computadora está conectada directamente a un dispositivo central llamado **concentrador**.[3] Las funciones del concentrador incluyen el redireccionamiento de la información de una computadora a una computadora específica o a todas las computadoras que forman la red. Como concentrador, es factible utilizar computadoras universales o dispositivos de red especializados. Esta topología de red tiene sus desventajas, por ejemplo: el alto costo del equipo de la red debido a la necesidad de adquirir dispositivos especializados para el nodo central. Además, las posibilidades de incrementar el número de nodos en la red están limitadas por el número de puertos disponibles en el concentrador. A veces tiene sentido construir la red utilizando varios concentradores conectados entre sí en forma jerárquica mediante enlaces del tipo estrella (figura 2.8*e*). La estructura resultante también se conoce como **estrella jerárquica** o **árbol**. En la actualidad, la estructura en árbol es la más común y se usa ampliamente tanto en LAN como en WAN.

La configuración en **bus común** es una versión especial de la topología en estrella (figura 2.8*c*). En este caso, el papel que desempeña el elemento central se asigna al cable pasivo al cual se encuentran conectadas varias computadoras de acuerdo con el diseño de una compuerta *OR alambrada*. La mayoría de las redes inalámbricas tienen la misma topología; sin embargo, en este caso el medio común de transmisión por radio desempeña el papel del bus común. La información se transmite a través del cable y se encuentra simultáneamente disponible en todas las computadoras conectadas a este cable. Las principales ventajas de este diseño son su bajo costo y su simplicidad para conectar nuevos nodos a la red. La desventaja más significativa de bus común es su baja confiabilidad, ya que cualquier defecto en el cable o en cualquiera de los conectores paraliza toda la red. Otra desventaja del bus común es su bajo desempeño, pues este método de conexión significa que solamente una computadora puede transmitir datos a través de la red a la vez. Por tanto, el ancho de banda del enlace de comunicación siempre se divide entre todos los nodos de la red. Hasta fechas recientes, el bus común fue una de las topologías más populares de las LAN.

---

[2] A menudo, el término **malla** se emplea para designar a las topologías totalmente conectadas o a las que se acercan mucho a éstas.

[3] En este caso, el término concentrador se utiliza en un sentido amplio, con el cual se quiere significar cualquier dispositivo con múltiples entradas capaz de trabajar como elemento central (por ejemplo, se puede usar un switch o un ruteador).

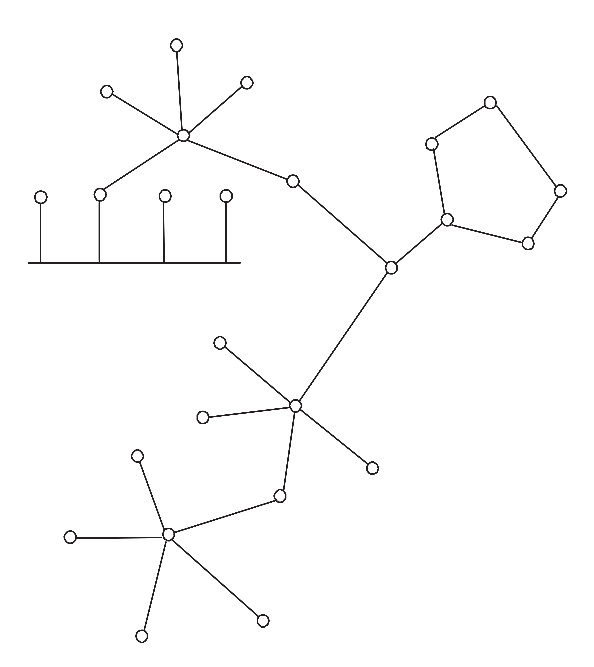


FIGURA 2.9 Red con topología híbrida.

Mientras que las redes pequeñas, en general, tienen una de las topologías típicas —estrella, anillo o bus común—, las redes de gran tamaño están caracterizadas por la presencia de conexiones arbitrarias entre computadoras. En dichas redes, uno puede distinguir fragmentos conectados de forma arbitraria (subredes) que cuentan con una topología típica. Por tanto, dichas redes se conocen como redes de **topología híbrida** (figura 2.9).

2.4.2 Direccionamiento de los nodos de red

Es necesario tener en cuenta el problema del direccionamiento cuando se conectan tres o más computadoras. Para ser precisos, esto es en realidad un problema de direccionamiento de sus interfases de red.[4] Una computadora puede contar con varias interfases de red; por ejemplo, para formar anillos físicos, cada computadora debe contar con al menos dos interfases de red para asegurar las conexiones con sus dos computadoras vecinas. Para crear una estructura de conectividad total que incluya N computadoras, es necesario equipar cada computadora con $N - 1$ interfases de red.

Por el número de interfases direccionadas, las direcciones de red pueden clasificarse como sigue:

- **Direcciones unidirigidas (unicast)**, que se utilizan para identificar las interfases individuales.
- **Direcciones multidirigidas (multicast)**, que identifican grupos de varias interfases. Los datos enviados a una dirección multidirigida se deberán entregar a todos los nodos que pertenezcan a ese grupo.

[4] A veces, en vez de usar el término preciso dirección de interfase de red, utilizaremos el vocablo simplificado dirección de nodo de red.

- Muchas tecnologías de red soportan las llamadas **direcciones multidifundidas (broadcast)**. Los datos enviados a dichas direcciones deberán entregarse a todos los nodos de la red.
- La nueva versión del protocolo Internet —IPv6— define un nuevo tipo de dirección: la **dirección a cualquier nodo de la red (anycast)**. De manera similar a las direcciones multidirigidas, estas direcciones definen grupos específicos de direcciones; sin embargo, los datos enviados a las direcciones de este tipo deben entregarse a cualquier dirección en el grupo en lugar de a todas las direcciones que pertenezcan a este grupo.

Las direcciones pueden ser **numéricas** (129.26.255.255) o **simbólicas** (sitio.dominio.com).

Las direcciones simbólicas (nombres) están diseñadas para identificar los nodos de red mediante un formato amigable; por tanto, en general tienen asociaciones semánticas. Dichas direcciones son fáciles de memorizar. Los nombres de red que se utilizan en las redes de gran tamaño pueden tener una estructura jerárquica, como **ftp-arch1.ucl.ac.uk**. Este nombre lleno de significado especifica que la computadora a la que se ha asignado tal número soporta el ftp-archive en la red de uno de los colegios de la Universidad de Londres (University College London o UCL). Asimismo, esta red tiene relación con la rama académica de Internet (AC) del Reino Unido (UK). Cuando se trabaja dentro de los límites de la red de la Universidad de Londres, este simbólico largo nombre resulta redundante. El nombre abreviado (ftp-arch1) es más apropiado que este nombre completo.

Los nombres simbólicos son adecuados para los humanos, sin embargo, debido a su formato variable y su longitud potencialmente significativa, su transmisión por medio de las redes es ineficaz.

> El conjunto completo de todas las direcciones válidas dentro de un método de direccionamiento específico se conoce con el nombre de **espacio de direcciones**.

Los espacios de direcciones pueden tener una organización **plana** (lineal; véase la figura 2.10) o **jerárquica** (figura 2.11).

En el primer caso, el espacio de direcciones no está estructurado. Un ejemplo típico de una dirección numérica plana es la llamada **dirección MAC**, diseñada para identificar de manera única y sin ambigüedades las interfases de red de las LAN. Dichas direcciones son utilizadas, en general, por el hardware; por tanto, se diseñan con el tamaño más corto posible. Como regla general, una dirección MAC se escribe en formato binario o hexadecimal (por ejemplo, 0081005e24a8). No se requiere trabajo manual para especificar las direcciones MAC, debido a que por lo regular los fabricantes de hardware las codifican en las tarjetas. Por esta razón, las direcciones MAC se conocen también con el nombre de **direcciones de hardware.** El uso de direcciones planas no representa una solución flexible, porque después de quitar el hardware de red (el adaptador de red, por ejemplo), la dirección de la interfase de red también se modifica.

Cuando se utiliza un método de **direccionamiento jerárquico** (figura 2.11), el espacio de direcciones se organiza como subgrupos anidados, los cuales definen la interfase de red específica mediante el acotamiento secuencial del rango de direcciones.

En la estructura de tres niveles del espacio de direcciones que se muestra en la figura 2.11, la dirección del nodo extremo está definida mediante los tres componentes que siguen: el **identificador de grupo** (K), el cual especifica el grupo al que pertenece un grupo específico; el **identificador de subgrupo** (L), y el **identificador de nodo** (n), el cual identifica de manera única el nodo dentro de su subgrupo. En la mayoría de los casos, el direccionamiento

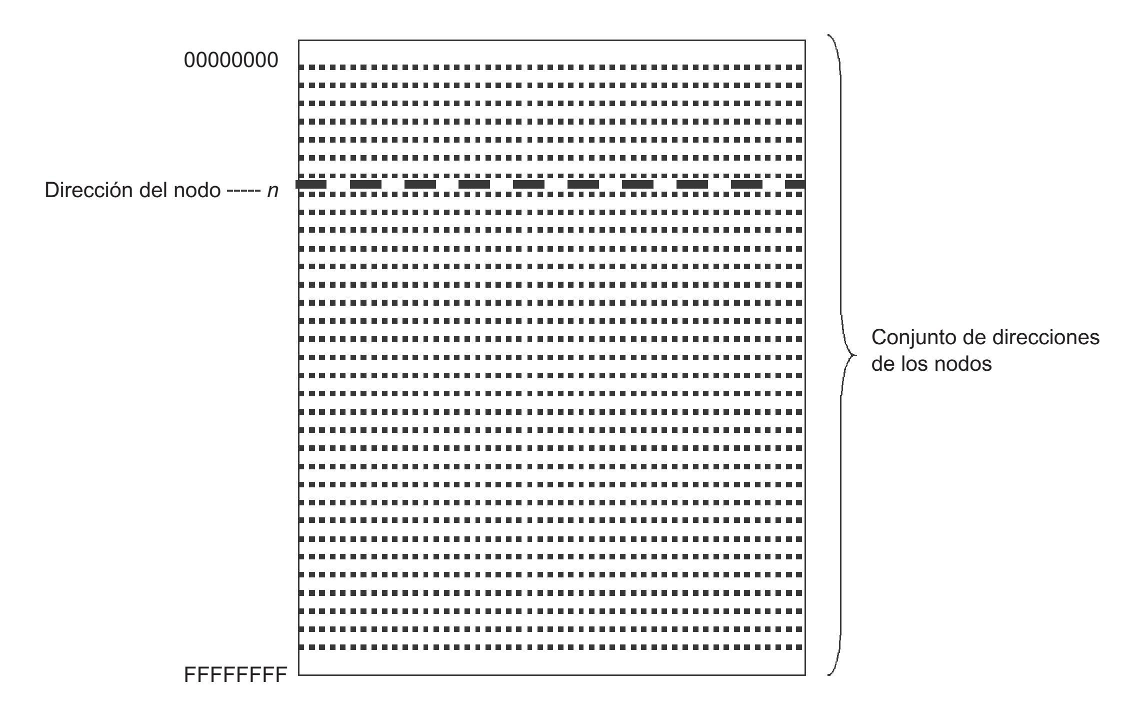


FIGURA 2.10 Organización plana del espacio de direcciones.

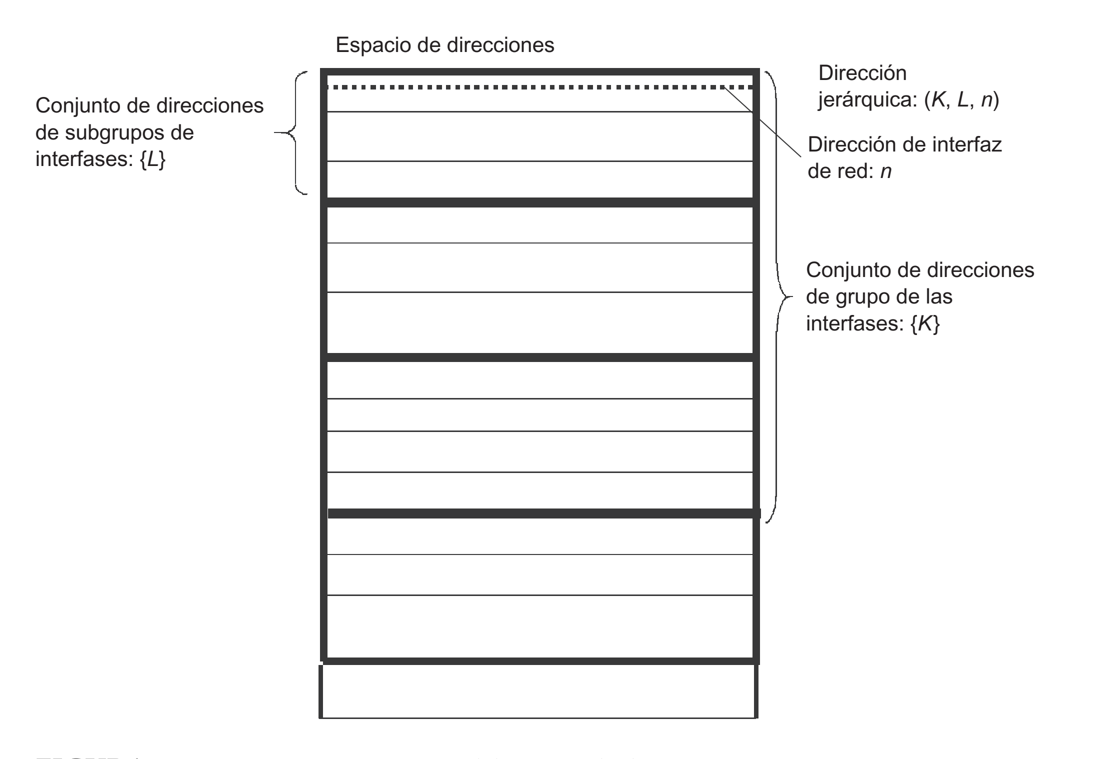


FIGURA 2.11 Estructura jerárquica del espacio de direcciones.

jerárquico es mucho más eficaz que la organización plana. En las redes grandes, con miles de nodos, el uso de direcciones planas da como resultado una subutilización significativa, debido a que los nodos extremos y el equipo de comunicaciones tienen que trabajar con tablas de

direcciones que cuentan con miles de registros. En contraste, el método de direccionamiento jerárquico en la transmisión de datos permite que solamente la parte más significativa (más hacia la izquierda) de la dirección (por ejemplo, *K*) se utilice hasta cierto momento. Después, con la finalidad de reducir el rango de direcciones, puede usarse la parte siguiente (*L*); por último, se puede emplear la parte menos significativa (*n*).

Las direcciones IP e IPX son ejemplos típicos de direcciones numéricas jerárquicas, las cuales soportan una jerarquía de dos niveles, donde una dirección se divide en la parte más significativa —el número de red— y la menos significativa —el número de nodo—. Dicha clasificación permite que la transmisión de mensajes entre redes esté basada en el número de red; a su vez, el número de nodo se utiliza solamente después de entregar el mensaje en la red de destino. Este método es similar al que usa el servicio postal en la entrega de correo. El nombre de la calle se consulta solamente después de que la carta ha sido enviada a la ciudad de destino.

En la práctica, varios métodos de direccionamiento se emplean de forma simultánea; por tanto, las interfases de red de la computadora pueden tener más de una dirección (o nombre). Cada dirección se usa cuando así conviene. Con la finalidad de convertir direcciones de una forma a otra, se utilizan protocolos especiales, llamados **protocolos de resolución de direcciones**.

Los usuarios direccionan a las computadoras mediante el uso de nombres simbólicos jerárquicos. En los mensajes transmitidos usando la red, estos nombres simbólicos se reemplazan de manera automática por direcciones numéricas jerárquicas. Mediante el uso de direcciones numéricas, los mensajes se transfieren de una red a otra y, después de entregar el mensaje a la red de destino, se usa la dirección plana de hardware de la computadora en lugar de la dirección numérica jerárquica.

Se pueden utilizar herramientas centralizadas o distribuidas para resolver el problema de establecer la correspondencia entre tipos de direcciones diferentes.

En el método centralizado existen computadoras dedicadas en la red, conocidas como *servidores de nombres*, que almacenan la tabla que compara los diferentes tipos de nombres (por ejemplo, nombres simbólicos y direcciones numéricas). Las demás computadoras solicitarán servidores de nombres con el fin de determinar el identificador numérico de una computadora específica utilizando su nombre simbólico.

Cuando se usa el método distribuido, cada computadora almacena su copia de los diversos tipos de direcciones asignados a ella. La computadora que necesita determinar la dirección plana de hardware correspondiente a la dirección jerárquica conocida envía una solicitud ampliamente difundida (broadcast) hacia la red. Todas las computadoras de la red comparan la dirección jerárquica especificada en este mensaje difundido con sus propias direcciones. La computadora que tenga la misma dirección enviará un mensaje de respuesta con la dirección plana de hardware requerida. Este método es utilizado por el protocolo de resolución de direcciones (ARP) de la pila de protocolos TCP/IP.

La ventaja del método distribuido es que no requiere una computadora dedicada, la cual, adicionalmente, a veces necesita la configuración manual de la tabla de mapeo de direcciones. Sin embargo, el método distribuido también tiene sus desventajas, la principal de las cuales es la necesidad de enviar mensajes difundidos que saturan la red debido a que éstos se reenvían a todos los nodos. Por tanto, el método distribuido se utiliza solamente en LAN pequeñas. En el caso de las LAN grandes es más común el método centralizado.

Hasta el momento, hemos centrado nuestra atención en las direcciones de las interfases de red de los nodos de red (es decir, computadoras o dispositivos de comunicación especializados). Sin embargo, ni la computadora ni el ruteador representan el punto de destino de los datos enviados a través de la red; más bien, es el software que corre en dichos dispositivos.

Por esta razón, la dirección de destino, además de incluir la información que identifica a la interfase del dispositivo de destino, también debe especificar la dirección del proceso para el cual están dirigidos los datos enviados a través de la red. Cuando los datos llegan a la interfase de red especificada en la dirección de destino, el software que corre en esa computadora debe reenviar los datos al programa que los requiera. Obviamente, la dirección del programa no tiene que ser única en toda la red, basta con asegurar que es única dentro de una computadora. Los **números de puerto** TCP y UDP que se utilizan en la pila de protocolos TCP/IP representan ejemplos de direcciones de programa.

2.4.3 Conmutación

Suponga que las computadoras se encuentran físicamente conectadas entre sí con una topología específica y que se ha seleccionado un método de direccionamiento determinado. Ahora debe resolverse el problema más importante: ¿qué método deberá utilizarse en la red para transmitir datos entre los nodos? Este problema resulta muy complejo cuando se utilizan topologías de red conectadas en forma parcial. En dicha situación, el intercambio de datos entre cualquier par de nodos (usuarios) seleccionados arbitrariamente debe llevarse a cabo a través de nodos de paso.

El proceso de conexión de nodos terminales a través de la red formada por nodos de paso se conoce con el nombre de **conmutación**. La secuencia de nodos en la trayectoria desde el nodo de origen al nodo de destino se llama **ruta**.

Por ejemplo, en la red que se muestra en la figura 2.12, los nodos 2 y 4, los cuales no están conectados directamente, deben transferir los datos a través de nodos de paso (es decir, los nodos 1 y 5). El nodo 1 debe transmitir datos de la interfase A a la B; a su vez, el nodo 5 debe llevar a cabo la misma operación transmitiendo datos de la interfase F a la B. En este ejemplo, la ruta puede describirse como sigue: 2-1-5-4, donde 2 es el nodo de origen, 1 y 5 son los nodos de paso y el nodo 4 es el nodo de destino.

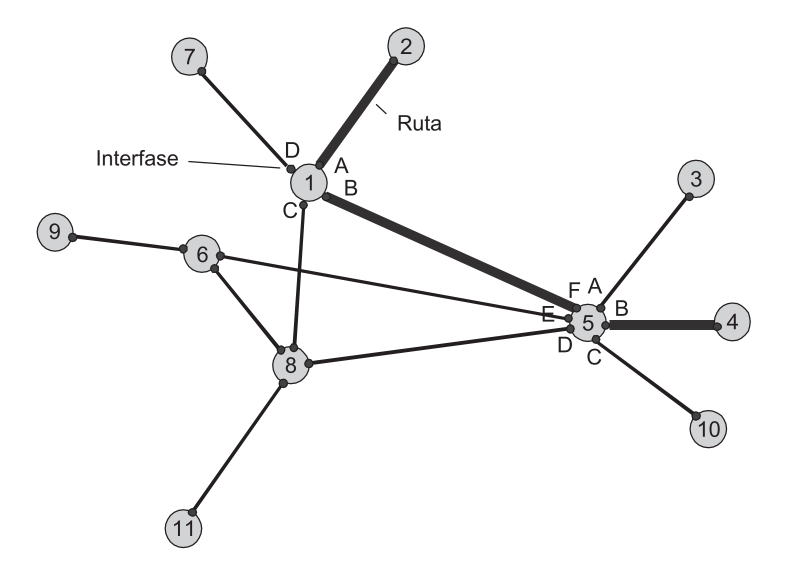


FIGURA 2.12 Conmutación a través de la red de nodos de paso.

2.5 PROBLEMA GENERALIZADO DE CONMUTACIÓN

PALABRAS CLAVE: conmutación, flujo de información o flujo de datos, etiqueta del flujo, métrica de enrutamiento, multiplexaje por división de tiempo (TDM) y multiplexaje por división de frecuencia (FDM), multiplexor, demultiplexor, conexión en fila india, árbitro, enlace compartido, medio compartido, conmutación de circuitos, conmutación de paquetes, direccionamiento de datos, red de conmutación.

En su forma más general, la función de conmutación puede representarse como el conjunto de tareas relacionadas entre sí que se mencionan en seguida:

- Determinación de los flujos de información para los que se deben definir rutas
- Enrutamiento de los flujos de información
- Envío de los flujos (es decir, reconocimiento del flujo y conmutación local en cada nodo de tránsito)
- Multiplexaje y demultiplexaje del flujo

2.5.1 Definición de flujo

Obviamente, es factible establecer varias rutas a través de un solo nodo de paso; por ejemplo, todos los datos que envía el nodo 4 (figura 2.12) deben pasar a través del nodo 5, así como todos los datos entrantes a los nodos 3, 4 y 10. Los nodos de paso deben ser capaces de reconocer los flujos de datos entrantes con el fin de reenviar a cada uno de ellos a la interfase que los enviará al nodo de destino requerido.

Flujo de información o de datos es la secuencia continua de datos relacionados mediante un conjunto de atributos comunes que la distingue del tráfico total de la red.

Por ejemplo, puede decirse que todos los datos que provienen de una computadora específica representan un solo flujo para el que la dirección origen sirve como atributo unificador. Los mismos datos pueden representarse como un conjunto de varios subflujos más pequeños, cada uno de los cuales utiliza la dirección de destino como un atributo diferenciador. Por último, cada uno de estos subflujos puede dividirse a su vez en flujos de datos generados por diferentes aplicaciones de red, como el correo electrónico, programas de copiado de archivo o servidores Web.

Los datos que conforman un flujo pueden representarse mediante unidades de datos: paquetes, tramas o celdas.

NOTA *Junto con los flujos de datos existen también conceptos como corriente de datos. En general, un flujo de datos tiene una velocidad variable, mientras que la velocidad de una corriente de datos es constante. Por ejemplo, cuando circula una página web a través de Internet, la carga ofrecida representa el flujo de datos; durante la difusión de música a través de Internet, dicha carga representa una corriente de datos. En las redes de datos, las velocidades irregulares son más comunes; por tanto, en la mayoría de los casos utilizaremos el término flujo. El vocablo corriente se usará solamente cuando sea necesario hacer énfasis en el carácter isócrono de este proceso.*

En el proceso de conmutación de datos, la dirección de destino es un atributo obligado. Con base en este atributo, todo el flujo de datos destinado al nodo de paso se divide en subflujos, cada uno de los cuales se envía a la interfase específica que corresponda a la ruta de envío de datos.

Las direcciones de origen y destino determinan un solo flujo para cada par de nodos terminales. Con mucha frecuencia, resulta de utilidad representar el flujo de datos entre dos nodos terminales como un conjunto de subflujos, cada uno de los cuales viaja a través de su ruta específica. El mismo par de nodos terminales puede llevar a cabo varias aplicaciones que interactúan entre sí utilizando la red. Al mismo tiempo, cada una de estas aplicaciones puede tener sus propios requerimientos para la red; en este caso, la selección de la ruta debe llevarse a cabo de acuerdo con los requerimientos de la aplicación. Por ejemplo, para un servidor de archivos, es importante que al enviar las grandes cantidades de datos transmitidos se utilice un enlace de comunicaciones que posea un gran ancho de banda. En un sistema de administración que envía mensajes cortos que deban procesarse de manera inmediata, la confiabilidad de los enlaces de comunicación, así como la existencia de un nivel mínimo de retardos en la ruta seleccionada representan aspectos de gran importancia. Además, aun para los datos que posean requerimientos similares para la red, será necesario establecer rutas con el fin de acelerar el procesamiento de datos mediante el uso en paralelo de los diferentes enlaces de comunicación.

Los atributos de los flujos pueden ser *globales* o *locales*. En el primer caso, éstos identifican sin ambigüedades el flujo dentro de los límites de toda la red; en el segundo, hacen lo mismo solamente dentro de los límites del nodo de paso específico. Un par de direcciones únicas de los nodos terminales representa un ejemplo del atributo global para la identificación de flujos. El ID de la interfase del nodo de paso específico al cual se han enviado los datos puede servir como un atributo que defina localmente el flujo dentro de un dispositivo específico. Para ilustrar estas definiciones, refiérase a la configuración de red que se muestra en la figura 2.9. En este ejemplo, el nodo 1 puede configurarse para transmitir todos los datos que provienen de la interfase D y llegan a la C. Especificar dicha regla facilita que el flujo de datos que proviene del nodo 2 pueda separarse del flujo de datos proveniente del nodo 7; asimismo, permite reenviarlos a través de nodos de red diferentes. En este caso, los datos provenientes del nodo 2 viajarán a través del nodo 5 y los provenientes del nodo 7 serán transmitidos a través del nodo 8.

Existe también un tipo específico de atributo de flujo llamado *etiqueta de flujo* que representa un número específico con el cual cuentan todos los datos del flujo. La etiqueta puede tener un valor global que identifique de manera única el flujo dentro de los límites de la red. En este caso, se asigna a las unidades de datos del flujo y nunca cambia a través de toda la ruta desde el nodo de origen hasta el nodo de destino. En algunos casos se utilizan etiquetas de flujos locales que, de manera dinámica, cambian sus valores cuando circulan de un nodo a otro.

Por tanto, el reconocimiento del flujo durante el proceso de conmutación se basa en atributos que, aparte de la *dirección de destino* obligada, pueden contener información tal como el identificador de una aplicación específica.

2.5.2 Enrutamiento

El problema del enrutamiento abarca dos tareas adicionales:

- Determinación de rutas
- Notificación a la red acerca de la ruta seleccionada

La resolución del problema de seleccionar la ruta para la transmisión de datos incluye determinar la secuencia de nodos de paso y sus interfases, a través de las cuales es necesario que circulen los datos con el fin de entregarlos a la dirección de destino. Determinar la ruta es una tarea compleja, especialmente cuando las configuraciones de red permiten la existencia de varias rutas entre un par de interfases de red que interactúan. Con mucha frecuencia, es necesario seleccionar solamente una ruta *óptima*[5] de acuerdo con un criterio específico. Se pueden utilizar varios criterios como criterio óptimo, por ejemplo: el ancho de banda nominal y la carga de los enlaces de comunicación, los retardos provocados por enlaces específicos, el número de nodos de paso y la confiabilidad de los enlaces de comunicaciones y de los nodos de paso.

Aun cuando solamente exista *una* posible ruta entre nodos terminales, encontrarla puede ser una tarea muy retadora en una topología de red bastante compleja.

La ruta puede ser determinada de manera empírica ("manualmente") por el administrador de la red, quien a menudo utiliza diferentes consideraciones que no pueden ser formalizadas. Entre las razones de seleccionar rutas específicas pueden estar las siguientes: requerimientos especiales de la red en función de tipos de aplicaciones específicos, la decisión de transmitir tráfico utilizando la red de un proveedor de servicios determinado, suposiciones relacionadas con las cargas pico en enlaces de red específicos y, por último pero no menos importante, consideraciones de seguridad.

Sin embargo, un método empírico para determinar rutas no es apropiado en redes de gran tamaño con topologías complejas. En dichas redes, es mejor utilizar métodos automáticos en la determinación de rutas.

Para lograr dicho objetivo, los nodos terminales y otros dispositivos de red cuentan con herramientas especializadas de software que organizan el intercambio mediante mensajes de servicio, permitiendo así que cada nodo de red obtenga su propia representación de la red. Después, con base en los datos recabados y utilizando diferentes tipos de software especializado, se determinan de manera automática las rutas más apropiadas.

Se pueden utilizar varios tipos de información acerca de la red para seleccionar la ruta óptima; sin embargo, cuando se resuelve este problema, con mucha frecuencia solamente se tiene en cuenta información de la topología de la red. Este método se muestra en la figura 2.13. Hay dos rutas para transmitir el tráfico entre los nodos terminales A y C: A-1-2-3-C y A-1-3-C. Si no se considera ninguna información acerca de la red excepto los enlaces entre sus nodos, será lógico seleccionar la ruta A-1-3-C.

Esta solución se encontró al minimizar un criterio seleccionado.

> El parámetro de la ruta que se utilizó para tomar esta decisión se llama **métrica de enrutamiento**.

En este caso, se usó como el criterio de minimización de la longitud de la ruta medida como el número de nodos de paso. La minimización de la métrica de enrutamiento es el método principal para la selección de la ruta.

---

[5] En la práctica, para reducir la cantidad de cálculos, se selecciona por lo regular una ruta racional muy cercana a la óptima, en vez de seleccionar la óptima en sentido matemático.

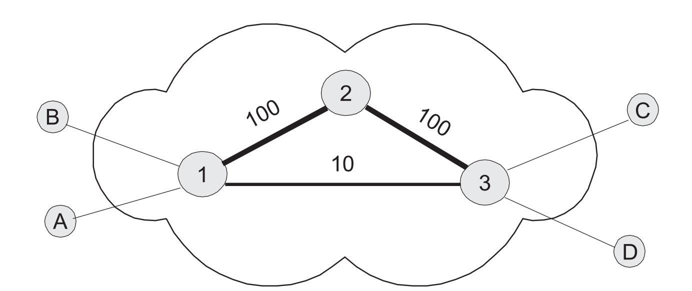


FIGURA 2.13 Selección de la ruta.

Sin embargo, es posible que esta selección se halle muy lejos de ser racional. El diseño que se presenta en la figura 2.13 muestra que los enlaces 1-2 y 2-3 están caracterizados por un ancho de banda de 100 Mbps y que el enlace 1-3 tiene un ancho de banda de 10 Mbps. Por tanto, si uno quisiera que la información viajara a la máxima velocidad, sería mejor seleccionar la ruta A-1-2-3-C, a pesar de que ésta tiene tres nodos de paso.

Por esa razón, se pueden seleccionar varias métricas para medir la longitud de la ruta, entre las que se incluyen el número de nodos de paso (como en el caso estudiado anteriormente), la longitud lineal de la ruta e incluso su costo en términos económicos. Para construir una métrica cuando la información debe viajar a su velocidad máxima, cada enlace está caracterizado por un valor inversamente proporcional a su ancho de banda. Para operar con números enteros, generalmente se selecciona alguna constante que sea mayor que los valores del ancho de banda de los enlaces de la red. Por ejemplo, si se selecciona el valor de 100 Mbps como dicha constante, la métrica de los enlaces 1-2 y 2-3 será igual que 1 y la métrica del enlace 1-3 será igual que 10. La métrica de enrutamiento es igual a la suma de las métricas de los enlaces que la forman; por tanto, la parte 1-2-3 de la ruta tiene un valor de la métrica de 2, y la parte 1-3 de la ruta tiene un valor de la métrica de 10. La ruta racional es la que tiene el valor de métrica más pequeño, es decir, la ruta A-1-2-3-C.

Dichas formas de seleccionar rutas consideran solamente la topología de la red, sin tener en cuenta la carga de tráfico de los enlaces de comunicación.[6] Al usar la analogía del tráfico de automóviles, se puede decir que hemos seleccionado la ruta utilizando un mapa, tomando en cuenta el número de ciudades de paso y el ancho de la carretera (esto último es análogo al ancho de banda del enlace) cuando se establecen las preferencias de la carretera. Sin embargo, no prestamos atención a los programas de radio y televisión que informan a los viajeros acerca de los congestionamientos de tráfico que se presentan en ese momento. Por tanto, es posible que nuestra solución esté muy alejada de ser la mejor, especialmente si un gran número de flujos de datos son transmitidos a través de la ruta A-1-2-3-C y la ruta A-1-3-C se encuentra prácticamente vacía.

Después de seleccionar la ruta (ya sea manual o automáticamente) es necesario informar a todos los dispositivos de la red la decisión que se ha tomado. Los mensajes que informan a los dispositivos de la red acerca de la ruta seleccionada deben entregar a cada dispositivo de paso una variación de la información siguiente: "Siempre que el dispositivo reciba datos relacionados con el flujo N, es necesario transferirlos a la interfase F para su posterior envío". El dispositivo procesa cada mensaje de enrutamiento de este tipo. Como resultado, el

[6] Los métodos que utilizan información acerca de la carga de trabajo actual en los enlaces de comunicaciones permiten encontrar rutas más eficaces; sin embargo, también originan que los nodos de la red intercambien información auxiliar de manera más intensa.

nuevo registro se coloca en la tabla de conmutación, donde los atributos locales y globales del flujo (por ejemplo, su etiqueta, el número de la interfase de entrada o la dirección de destino) se comparan con el número de la interfase a la que el dispositivo debe reenviar los datos relacionados con este flujo.

La tabla 2.1 es un fragmento de la tabla de conmutación que contiene los registros que informan al nodo que reenvíe el flujo M a la interfase G, el flujo N a la interfase F y el flujo P a la interfase H.

TABLA 2.1 Fragmento de la tabla de conmutación

Atributos de los flujos	Redirección de los datos (número de interfase o siguiente dirección del nodo)
M	G
N	F
P	H

Como es natural, las descripciones en detalle de la estructura de mensajes de enrutamiento y el contenido de la tabla de conmutación dependen de la tecnología de red específica; sin embargo, estas características especiales no modifican la esencia de los procesos que se consideran.

La transmisión de la información de enrutamiento a los dispositivos de paso, como la selección de la ruta, puede llevarse a cabo en forma manual o automática. Los administradores de red pueden establecer rutas específicas mediante la configuración del dispositivo en forma manual, por ejemplo, conectando físicamente pares de interfases de entrada y salida durante un tiempo largo. Esto es similar a las operadoras telefónicas que trabajaban con las primeras centrales telefónicas; además, los administradores de red podrán editar en forma manual la tabla de conmutación si ingresan los registros que se requieran.

Sin embargo, la topología de la red y los flujos de información pueden ser modificados. Estos cambios, por ejemplo, pueden ser originados por factores como la falla de algunos nodos o la adición de nuevos nodos de paso; además, las direcciones de red pueden cambiar o se pueden definir nuevos flujos. En consecuencia, es necesario un método flexible para resolver los problemas asociados con la determinación y especificación de las rutas, método que implica el análisis permanente del estado de la red y la actualización de las rutas y tablas de conmutación. En dichos casos, determinar la ruta no es fácil sin el uso de herramientas complejas de software y hardware.

2.5.3 Direccionamiento de datos

Cuando se han determinado y almacenado las rutas en las tablas de conmutación de los nodos de paso, todo se encuentra listo para llevar a cabo la tarea principal: la transmisión de datos entre los nodos terminales o la conmutación de los nodos terminales.

Por cada par de nodos terminales, dicha operación puede representar una combinación de varias operaciones locales de conmutación (su número corresponde a la cantidad de nodos de paso). Esto es, el emisor debe proporcionar datos a la interfase específica desde la cual la ruta seleccionada se originó y, en función de esto, los demás nodos de paso deben redirigir los datos de una interfase a otra. En otras palabras, los nodos de paso deben llevar a cabo la *conmutación de la interfase local.*

El dispositivo diseñado para realizar la función de conmutación se conoce con el nombre de **switch** (**interruptor)** (figura 2.14).

Sin embargo, antes de llevar a cabo la conmutación, el switch tiene que reconocer el flujo. Con el fin de llevar a cabo esto, debe analizar los datos entregados para encontrar atributos de ciertos flujos de datos especificados en la tabla de conmutación. Si se encuentra una coincidencia, estos datos se reenvían a la interfase definida por ellas en la ruta.

IMPORTANTE *Los términos conmutación, tabla de conmutación y switch pueden interpretarse de manera ambigua en las redes de telecomunicaciones. Ya hemos definido el vocablo conmutación como el proceso de conexión de nodos de red vía nodos de paso. El mismo término se utiliza para designar la conexión de las interfases dentro de un nodo de paso específico. El switch, en un sentido amplio, es cualquier dispositivo capaz de llevar a cabo la función de conmutación de flujos de datos entre interfases. La operación de conmutación puede llevarse a cabo de acuerdo con diferentes reglas y algoritmos. Algunos métodos de conmutación y sus correspondientes tablas de conmutación y dispositivos tienen nombres especiales. Por ejemplo, en tecnologías a nivel de red como IP e IPX, se utilizan diferentes términos para designar conceptos similares: enrutamiento, tabla de enrutamiento y ruteador. En Ethernet, la tabla de conmutación generalmente se llama tabla de direccionamiento. A otros tipos especiales de conmutación y sus dispositivos correspondientes se les han asignado los mismos nombres: conmutación, tabla de conmutación y switch, que se utilizan en un sentido restringido, por ejemplo, para el switch y la conmutación LAN. En las redes telefónicas, las cuales aparecieron mucho antes que las redes de computadoras, es característica una terminología similar. Aquí, el switch es sinónimo de central telefónica. Debido a la edad y prevalencia de las redes telefónicas, el término switch en telecomunicaciones se usa con mucha frecuencia como sinónimo de central telefónica.*

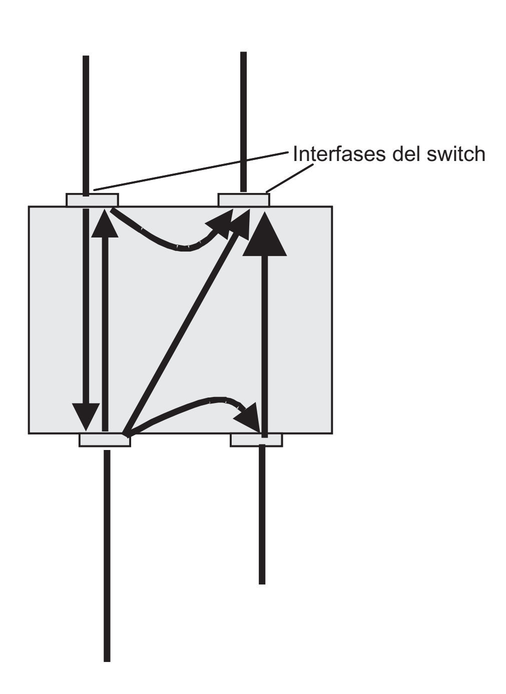


FIGURA 2.14 Switch.

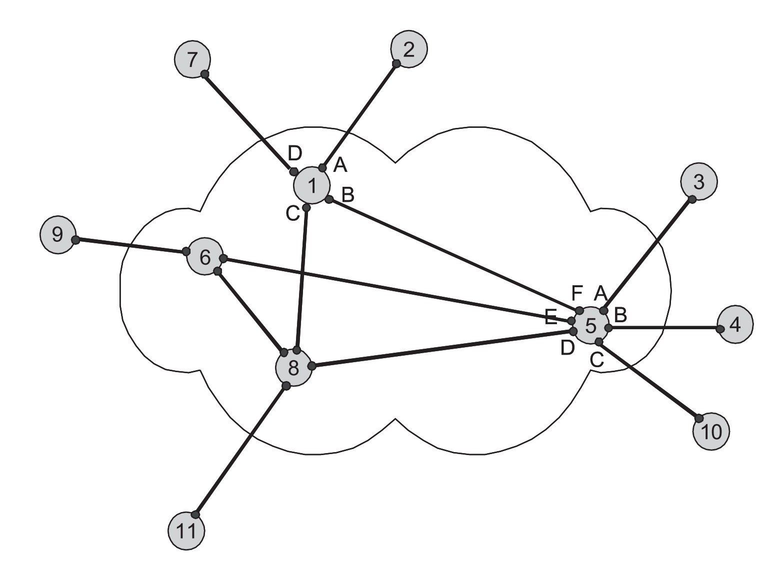


FIGURA 2.15 Red de conmutación.

Tanto los dispositivos especializados como las computadoras universales con software de conmutación incorporado pueden hacer las veces de un switch. La computadora puede combinar las funciones de conmutación con la funcionalidad normal de nodo terminal; sin embargo, en la mayoría de los casos resulta mucho más práctico asignar a nodos de red específicos para llevar a cabo las funciones de conmutación. Estos nodos forman la red de conmutación a la que están conectados los demás nodos. La figura 2.15 muestra una red de conmutación formada por los nodos 1, 5, 6 y 8, a los cuales se encuentran conectados los nodos terminales 2, 3, 4, 7, 9 y 10.

2.5.4 Multiplexaje y demultiplexaje

Para determinar a qué interfase reenviar los datos entrantes, el switch debe determinar con qué flujo están relacionados. Esta tarea ha de resolverse independientemente de si se entrega un flujo "puro" o "mezclado" a la entrada del switch. El flujo "mezclado" es el resultado de la combinación de varios flujos de datos. En este caso, la función del reconocimiento del flujo se complementa con la tarea de demultiplexaje, o la separación del flujo agregado resultante en varios flujos componentes.

Como regla general, la operación de conmutación está acompañada de la de multiplexaje inverso, durante la cual el flujo agregado se crea a partir de flujos de datos independientes. Este flujo agregado podrá transmitirse si se utiliza un solo enlace físico de comunicaciones.

Las operaciones de multiplexaje y demultiplexaje tienen la misma importancia que la conmutación; sin ellas, sería necesario proporcionar un enlace independiente para cada flujo. Esto, a su vez, resultaría en un gran número de enlaces paralelos en una red, lo cual neutralizaría todas las ventajas de la red parcialmente conectada.

La figura 2.16 muestra un fragmento de red formado por tres switches. El switch 1 tiene cinco interfases de red. Considere lo que pasa en la interfase **int.1**, la cual recibe los datos entrantes que provienen de tres interfases: **int.3**, **int.4** e **int.5**. Es necesario enviar todos estos datos a través de un enlace común (es decir, llevar a cabo la operación de multiplexaje). El multiplexaje asegura la disponibilidad de enlaces físicos para diferentes sesiones de red entre los nodos terminales de la red.

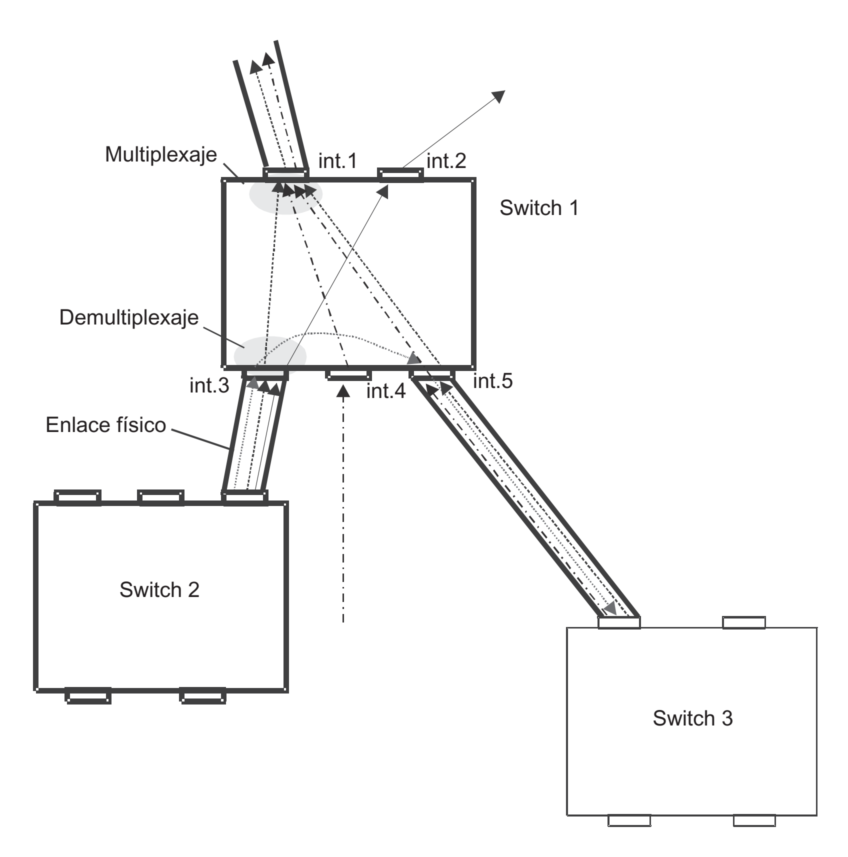


FIGURA 2.16 Operaciones de multiplexaje y demultiplexaje durante la conmutación de flujos.

Existen varios métodos para multiplexar flujos en un solo enlace físico, de los cuales los más importantes son el **multiplexaje por división de tiempo (TDM)** y el **multiplexaje por división de frecuencia (FDM)**. Cuando se utiliza TDM, cada flujo cuenta con el enlace a su disposición de forma permanente o a espacios de tiempo arbitrarios y al transmitir sus datos utiliza este enlace. Cuando se usa FDM, cada flujo transmite sus datos en un rango de frecuencias que se le asignan.

La tecnología de multiplexaje debe permitir que el receptor de dichos flujos agregados lleve a cabo una operación inversa: demultiplexar los datos en flujos independientes. Por ejemplo, en la interfase int.3, el switch demultiplexa el flujo agregado en tres flujos componentes. El primero es enviado a la interfase int.1, el segundo a la **int.2** y el tercero a la **int.5**. En cuanto a la interfase **int.2**, no es necesario realizar multiplexaje y demultiplexaje, pues esta interfase es para uso exclusivo de un solo flujo. En la práctica, tanto el multiplexaje como el demultiplexaje pueden efectuarse, de manera simultánea, en toda interfase que soporte el modo dúplex.

Cuando todos los flujos de información entrantes se conmutan a una sola interfase de salida, donde se multiplexan en un solo flujo agregado y se envían por el enlace común, el switch se conoce como *multiplexor*. La figura 2.17*a* muestra un switch de este tipo. Un switch que tenga una sola interfase de entrada y varias de salida se conoce como *demultiplexor* (figura 2.17*b*).

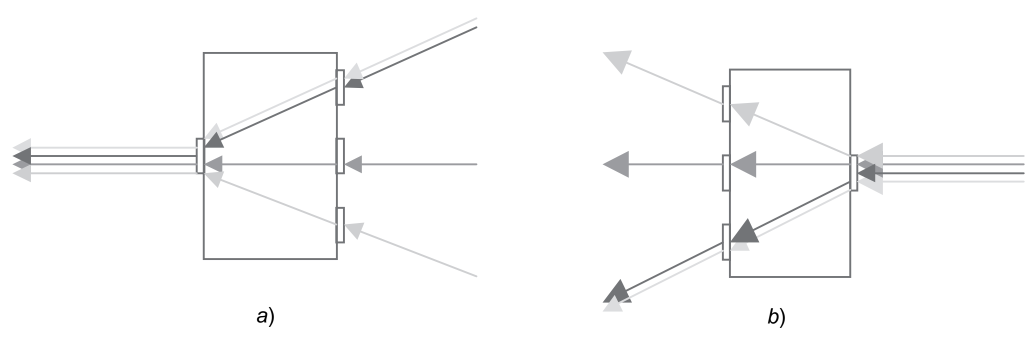


FIGURA 2.17 Multiplexor y demultiplexor.

2.5.5 Medio compartido

El **número de nodos de red conectados a un enlace de datos** representa otro parámetro de un enlace. En los ejemplos dados, solamente dos nodos que interactúan entre sí (para ser más precisos, dos interfases) se conectaron a un enlace de comunicaciones (figura 2.18*a* y *b*). En las redes de telecomunicaciones se utiliza otro tipo de conexión en la que varias interfases están conectadas a un solo enlace (figura 2.18*c*). Tales conexiones múltiples de varias interfases resultan en la tecnología de bus común que ya se estudió, a menudo conocida como *conexión en fila india*. En todos esos casos, uno tiene que resolver el problema de compartir el enlace entre las múltiples interfases.

La figura 2.18 muestra diferentes métodos para compartir el enlace entre las interfases múltiples. En la figura 2.18*a*, los switches S1 y S2 están conectados mediante dos enlaces físicos unidireccionales (es decir, cada enlace puede transmitir información en una sola dirección). En este caso, la interfase de transmisión está activa y el medio de transmisión se encuentra totalmente bajo el control de esta interfase, mientras que la interfase pasiva sólo recibe datos. *En este caso, no hay problema alguno para compartir el enlace entre las dos interfases.* Sin embargo, observe que aún es necesario resolver el problema del multiplexaje de datos en dicho enlace. En la práctica, dos enlaces unidireccionales que implementen una conexión *full*-dúplex entre dos dispositivos se consideran un solo enlace dúplex, y las dos interfases de un solo dispositivo se interpretan como los componentes de transmisión y recepción de la misma interfase.

En la figura 2.18*b*, los switches S1 y S2 están conectados mediante un enlace capaz de transmitir datos en ambas direcciones, aunque solamente uno a la vez. Es *necesario implementar un mecanismo de acceso sincronizado* de las interfases S1 y S2 para dicho enlace. La configuración que se muestra en la figura 2.18*c*, en la que más de dos interfases se encuentran conectadas al enlace de comunicaciones formando un bus común, representa una generalización de este caso.

El enlace físico proporcionado para su uso simultáneo por varias interfases se conoce como **enlace compartido**.[7] Con mucha frecuencia se utiliza otro término: **medio compartido**. Los enlaces de comunicaciones compartidos no solamente se utilizan en enlaces de switch a switch, sino también en enlace de computadora a switch y de computadora a computadora.

Existen varios métodos para resolver la tarea de organizar múltiples accesos a enlaces de comunicaciones compartidos. Algunos de ellos utilizan una técnica centralizada en la que

[7] Es necesario destacar que el término medio de transmisión compartido se relaciona tradicionalmente con compartir el enlace entre las interfases y prácticamente nunca se utiliza para describir cómo se comparte el enlace entre los flujos (es decir, el multiplexaje-demultiplexaje).

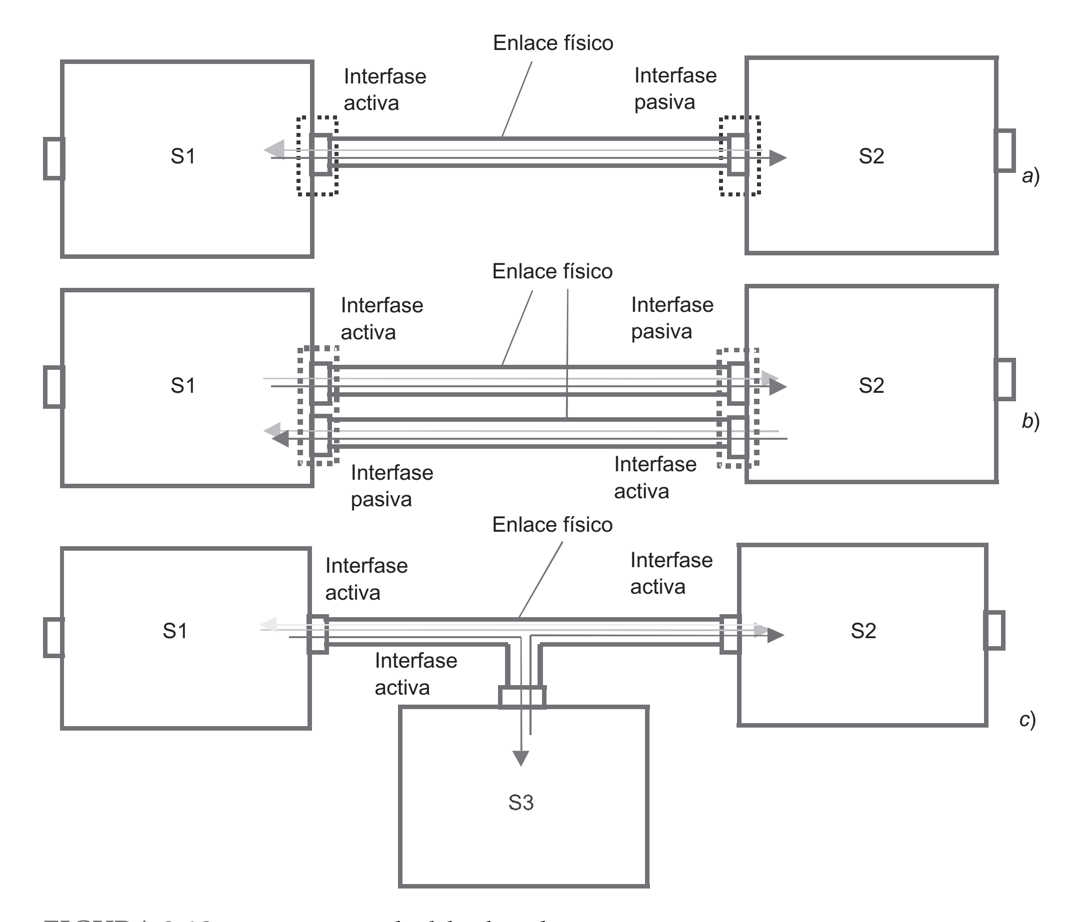


FIGURA 2.18 Uso compartido del enlace de comunicaciones.

un dispositivo especial llamado **árbitro** controla el acceso; otros métodos se basan en un esquema descentralizado. Los problemas asociados con compartir líneas de conexión entre módulos diferentes también se presentan dentro de una computadora. Un buen ejemplo de esto es el acceso al bus del sistema, el cual es controlado por el procesador o por un árbitro especial. La organización del acceso compartido a los enlaces de comunicaciones en las redes posee características especiales debido al tiempo significativamente más prolongado que se requiere para propagar las señales. Debido a lo anterior, los procedimientos para coordinar el acceso a un enlace de comunicaciones requieren prolongados espacios de tiempo y resultan en una disminución significativa del desempeño de la red. Por tanto, compartir el medio de transmisión prácticamente nunca se aplica en las WAN.

En las LAN, compartir el medio se aplica más a menudo debido a la simplicidad y eficiencia de su implantación. Este método se utiliza en Ethernet, la cual es la tecnología LAN que más prevalece en la actualidad, así como en las tecnologías *Token Ring* y FDDI, que fueron populares en el pasado.

Sin embargo, en años recientes, afloró otra tendencia: suprimir el medio compartido, aun en las LAN. La reducción en precio, la cual es la principal ventaja de este esquema, representa una disminución del desempeño de la red.

IMPORTANTE *Las redes con un medio de transmisión compartido formadas de un gran número de nodos siempre trabajarán a una velocidad menor que las redes similares con enlaces*

de conexión individuales punto-a-punto, ya que el ancho de banda de un enlace de comunicaciones compartido se divide entre las diferentes computadoras que forman la red.

No obstante, el acceso compartido a las líneas de comunicaciones se conserva no sólo en las tecnologías clásicas de red, sino también en varias tecnologías nuevas diseñadas para LAN. Por ejemplo, los diseñadores de la tecnología Gigabit Ethernet, la cual fue aceptada como un nuevo estándar en 1998, ya incluye el modo de compartimiento del medio de transmisión en sus especificaciones, así como el modo de enlaces individuales de conexión.

2.5.6 Tipos de conmutación

La complejidad de las soluciones técnicas al problema generalizado de conmutación constituye la base de cualquier tecnología de red. En general, la solución de **cada** tarea de conmutación particular depende de las soluciones seleccionadas para las **demás** tareas de este conjunto. La lista de tareas de conmutación incluye lo siguiente:

- Determinación de flujos y rutas apropiadas
- Construcción de tablas de conmutación
- Reconocimiento de flujos
- Transferencia de datos entre diferentes interfases del mismo dispositivo
- Multiplexaje/demultiplexaje de flujos
- Compartimiento del medio de transmisión

Entre los métodos posibles para resolver el problema de conmutación se pueden distinguir los dos métodos fundamentales siguientes:

- *Conmutación de circuitos.*
- *Conmutación de paquetes.*

Las redes de conmutación de circuitos tienen una larga historia, pues se originaron a partir de las primeras redes telefónicas. Las redes de conmutación de paquetes son relativamente nuevas y aparecieron a finales de la década de 1960 como resultado de experimentos con las primeras WAN. Cada una de estas redes tiene sus ventajas y desventajas; sin embargo, de acuerdo con el pronóstico a largo plazo de los especialistas, el futuro residirá en la tecnología de conmutación de paquetes, porque es más flexible y universal.

EJEMPLO *Simplifiquemos la descripción resumida del modelo generalizado de conmutación utilizando el ejemplo de la operación del servicio postal.*

1. *El servicio postal trabaja con flujos. En este caso, los flujos se forman mediante artículos del correo. Por lo general, la dirección del receptor sirve como el atributo del flujo principal. Con el fin de simplificar, considere que el país de destino es el único atributo de la dirección: India, Noruega, Brasil, Rusia, etc. A veces, un requerimiento específico relacionado con la confiabilidad o velocidad de entrega sirve como atributo adicional del flujo. Por ejemplo, si un artículo de correo con destino a Brasil tiene la etiqueta "AIRMAIL/PAR AVION", un subflujo que debe entregarse por correo aéreo se separará del flujo de correo con destino a Brasil.*

2. *Por cada flujo, el servicio postal tiene que definir una ruta que pasará a través de una serie de oficinas postales, análogas a los switches de la red. La larga historia de la operación del servicio postal ha dado como consecuencia rutas predefinidas para la mayoría de las direcciones de destino. Pueden aparecer nuevas rutas, lo cual puede tener como resultado la aparición de nuevos sistemas de transporte o de cambios o trastornos económicos y políticos. Después de seleccionar una nueva ruta, es necesario informar a toda la red de oficinas postales acerca de dicha ruta. Obviamente, estas acciones son similares a las que se llevan a cabo en la operación de una red de telecomunicaciones.*
3. *La información acerca de las rutas seleccionadas para la entrega del correo se presenta en cada oficina postal en la forma de una tabla que especifica la correspondencia entre el país de destino y la oficina postal siguiente en la secuencia de entregas. Por ejemplo, en la oficina postal central de Bruselas, todos los artículos del correo que se entregarán en India pueden dirigirse a la oficina postal central de Moscú. Dicha tabla de enrutamiento postal es análoga a la tabla de conmutación de una red de comunicaciones.*
4. *La operación de cada oficina postal es similar a la de un switch. Todos los artículos postales de los clientes o de otras oficinas postales se clasifican, lo cual significa que se lleva a cabo un reconocimiento del flujo. Después de llevarse a cabo lo anterior, los artículos de correo que pertenecen al mismo flujo se guardan en un paquete común para el cual la siguiente oficina postal se define de acuerdo con la tabla de conmutación.*

RESUMEN

- Para permitir que los usuarios de red accedan a los recursos de otras computadoras como discos, impresoras y plotters, es necesario equipar a todas las computadoras de la red con herramientas especiales. Las funciones de transmisión de datos en un enlace de comunicación en cada computadora se llevan a cabo en coordinación con hardware especial: la tarjeta de interfase de red (nic) y el driver de la nic, el módulo de software que la controla. Las tareas de alto nivel, como la generación de solicitudes a recursos y la atención de éstas, las llevan a cabo los módulos cliente y servidor del so, respectivamente.
- Aun en la red más sencilla, que solamente tenga dos computadoras, existen problemas en la transmisión de datos utilizando enlaces de comunicación, como la codificación y modulación, la sincronización de los dispositivos emisor y receptor y el control de errores de los datos transmitidos.
- Tanto la carga ofrecida, la velocidad de transmisión de la información o uso de la red, como la capacidad y el ancho de banda son características importantes relacionadas con la transmisión de tráfico a través de canales físicos.
- Cuando se conectan más de dos computadoras a una red, se *deben resolver* problemas asociados con la selección de la topología. *Dichas topologías son: totalmente conectadas, estrella, anillo, bus común, árbol jerárquico e híbrida.* El método de direccionamiento puede ser plano o jerárquico, numérico o simbólico. Usted también tiene que seleccionar los mecanismos de conmutación y el de compartimiento de los enlaces de comunicaciones.
- En las redes con conectividad parcial, las conexiones entre los usuarios se establecen mediante la conmutación (es decir, al conectarse a través de una red de nodos de paso). En este caso, es necesario resolver los problemas siguientes: el flujo de datos y la definición de la ruta, el envío de datos en cada nodo de paso y el multiplexaje y demultiplexaje del flujo.

► Entre las diferentes soluciones al problema de conmutación que existen, se pueden distinguir los métodos fundamentales siguientes: *conmutación de circuitos* y *conmutación de paquetes.*

PREGUNTAS DE REPASO

1. ¿Qué información se transmite al utilizar el enlace que conecta las interfases externas de la computadora con el dispositivo periférico?
2. ¿Qué componentes posee la interfase de un dispositivo?
3. ¿Qué tareas lleva a cabo el sistema operativo cuando intercambia datos con los dispositivos periféricos?
4. ¿Qué acciones realiza típicamente el driver de un dispositivo periférico?
5. Defina el término *topología.*
6. ¿A qué tipo de topología se puede atribuir la estructura constituida por nodos conectados entre sí formando un triángulo?
7. ¿A qué tipo de topología se puede atribuir la estructura constituida por nodos conectados entre sí en forma de cuadrado?
8. ¿A qué tipo de topología se puede atribuir la estructura formada por tres nodos conectados secuencialmente (el último nodo no está conectado al primero)?
9. La topología de bus común es un caso particular de:
   a) Totalmente conectados
   b) Anillo
   c) Estrella
10. ¿Qué topología se caracteriza por poseer una gran confiabilidad?
11. ¿Qué topología es la más comúnmente utilizada en las LAN actuales?
12. ¿Cuáles son los requisitos que debe cumplir un sistema de direccionamiento?
13. ¿A qué tipo de direccionamiento pueden atribuirse las direcciones que se listan a continuación?
    www.olifer.net
    20-34-a2-00-c2-27
    128.145.23.170
14. ¿Qué diferencias existen entre un flujo y una corriente?
15. ¿Qué atributos pueden utilizarse como característicos de un flujo?
16. Describa los principales métodos y criterios que se utilizan al seleccionar una ruta.
17. ¿Cuáles de los enunciados siguientes pueden ser verdaderos en algunos casos?
    a) Las rutas se configuran como fijas en los switches mediante la conexión de pares de interfases.
    b) Las rutas las define el administrador de la red y se ingresan a una tabla especial en forma manual.
    c) La tabla de enrutamiento se ingresa al switch en la planta de manufactura.
    d) El hardware y el software de la red crean la tabla de enrutamiento de manera automática.
    e) Cada switch tiene una tabla de enrutamiento especial almacenada en él.
18. ¿Cuáles de estos dispositivos —una central telefónica automática, un ruteador, un puente o un multiplexor— se pueden considerar switches?
19. ¿Qué métodos se utilizan en el multiplexaje?
20. Describa la diferencia entre compartir un medio de transmisión y el multiplexaje.

PROBLEMAS

1. Describa los principales problemas que deben resolverse, con el fin de asegurar el intercambio de información entre cualquier par de suscriptores en todo tipo de red de comunicaciones.
2. Explique de qué forma la división del tráfico común hace posible optimizar el control de un sistema de transporte urbano en varios flujos independientes.
3. Suponga que existen varias rutas entre los nodos A y B de una red. Considere las ventajas y desventajas de las variantes de la transmisión de datos entre dichos nodos:
   - ¿Utiliza todas las rutas existentes para la transmisión de datos en paralelo mejor que transmitir todos los datos a través de una única ruta óptima de acuerdo con un criterio específico?
   - Usa algunas de las rutas posibles y comparte la transmisión de datos entre ellas. ¿Qué regla puede aplicarse con el fin de definir la ruta necesaria para enviar el paquete siguiente?

3

CONMUTACIÓN DE CIRCUITOS Y DE PAQUETES

DESCRIPCIÓN DEL CAPÍTULO

3.1 INTRODUCCIÓN

En este capítulo continuaremos con nuestra investigación acerca de los principios generales de la conmutación en las redes de telecomunicaciones. Concentrémonos en primera instancia en una descripción y comparación detalladas de los dos principios fundamentales de la conmutación: la conmutación de circuitos y la conmutación de paquetes.

La conmutación de circuitos apareció mucho antes que la de paquetes. Este principio tiene su origen en las primeras redes telefónicas. La restricción principal del principio de conmutación de circuitos es la imposibilidad de la redistribución dinámica del ancho de banda del enlace físico.

El principio de la conmutación de paquetes fue inventado por los diseñadores de las redes de computadoras. Dicho principio tiene en cuenta las características del tráfico de datos de las computadoras (como las ráfagas) y representa el método de conmutación, el cual es más eficaz en las redes de computadoras, más que los métodos tradicionales de conmutación de circuitos utilizados en las redes telefónicas.

Sin embargo, las ventajas y desventajas de cualquier tecnología de red son relativas. El uso de la memoria búffer en los switches de las redes de conmutación de paquetes permite usar de modo eficiente el ancho de banda del enlace cuando se transmite tráfico en ráfagas. Sin embargo, provoca retardos arbitrarios en la entrega de paquetes. Estos retardos representan una desventaja para el tráfico en tiempo real, el cual ha sido transmitido tradicionalmente mediante una técnica de conmutación de circuitos.

En este capítulo se estudian tres métodos de envío de paquetes que se usan en las redes de conmutación de paquetes: transmisión de datagramas, transmisión orientada a la conexión y la técnica de circuitos virtuales.

Por último, este capítulo concluye con el estudio del principio de medios compartidos, el cual se utiliza ampliamente en las LAN.

3.2 CONMUTACIÓN DE CIRCUITOS

PALABRAS CLAVE: conmutación de circuitos, establecimiento de la conexión, bloqueo de la solicitud de establecimiento, tráfico en tiempo real, ancho de banda garantizado, multiplexaje, canal agregado, subcanal, suscriptor, multiplexaje por división de frecuencia, multiplexaje por división de tiempo, tráfico en ráfagas, coeficiente de pulsación del tráfico.

En primera instancia, considere la conmutación de circuitos en su forma más simplificada, la cual aclarará la idea fundamental de este método. Como se muestra en la figura 3.1, una red conmutada está formada por switches conectados entre sí por medio de enlaces de comunicación. Cada enlace se caracteriza por poseer el mismo ancho de banda.

Cada nodo terminal (usuario) está conectado a la red mediante el uso de un dispositivo terminal, que envía datos hacia la red a una velocidad constante igual que el ancho de banda del enlace. Si la carga ofrecida en un tiempo es menor que el ancho de banda del enlace, el dispositivo terminal continuará *alimentando* la red con un flujo de datos constante, rellenando la información útil para el usuario con espacios *vacíos* insignificantes (figura 3.2). El dispositivo terminal *sabe* que parte del flujo de datos contiene información útil y parte es sólo información que no se utiliza. El dispositivo terminal de recepción debe eliminar la información que no es significativa, así como proporcionar al usuario solamente los datos enviados hacia la red por el emisor.

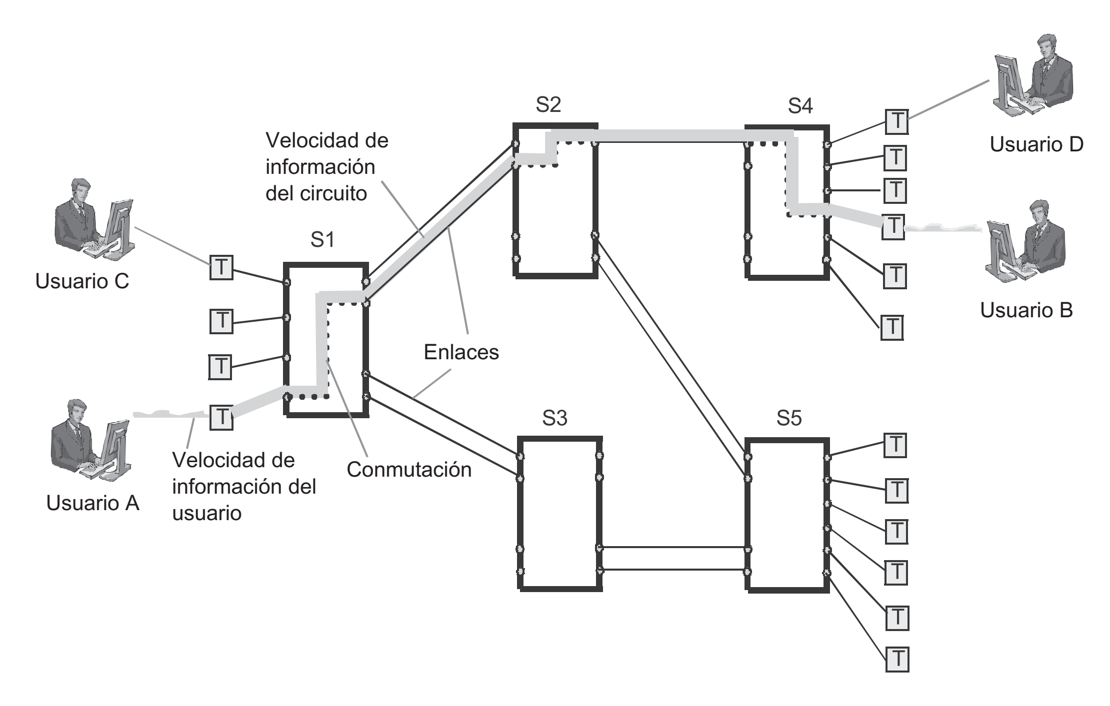


FIGURA 3.1 Conmutación de circuitos sin multiplexaje.

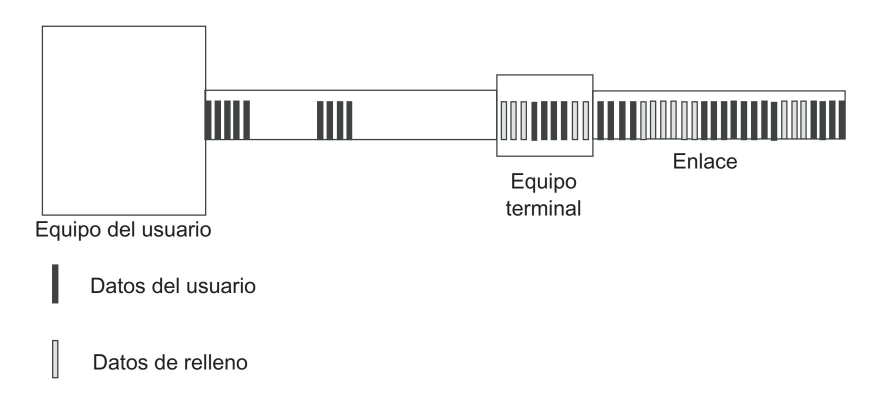


FIGURA 3.2 Complementación del flujo con el ancho de banda del enlace.

Como la mayoría de la gente está acostumbrada a las redes telefónicas, las cuales son los ejemplos más representativos de las redes de conmutación de circuitos, nuestra explicación estará complementada con referencias a los aspectos específicos característicos de la telefonía.

3.2.1 Establecimiento de la conexión

El intercambio de datos comienza después de que se ha **establecido la conexión**.

Suponga que dos suscriptores telefónicos (A y B) desean intercambiar información. Antes de enviar los datos a la red (es decir, iniciar una conversación), el suscriptor A envía la *solicitud* a la red de conmutación. En dicha solicitud, es necesario especificar la dirección (es

decir, el número telefónico) del suscriptor B. El objetivo de enviar esta solicitud es establecer la conexión entre los suscriptores A y B con un canal de información, cuyas propiedades sean similares a las de un enlace continuo de comunicaciones. Éste transmite datos a lo largo de toda la longitud del enlace a una velocidad constante, lo cual significa que los *switches de paso no necesitan almacenar datos de usuario.*

Con el fin de crear dicho enlace, la solicitud debe pasar a través de una secuencia de switches desde A hasta B, asegurándose de que estén disponibles todas las secciones requeridas de la ruta (enlaces de comunicaciones). Además de lo anterior, para establecer la conexión de modo exitoso, el nodo terminal B debe estar libre (es decir, no debe estar ocupado en otra conexión establecida). Para establecer la conexión, cada uno de los switches a lo largo de la trayectoria de A hasta B almacena la información que reserva la sección apropiada de la ruta para la conexión A-B. En cada switch se lleva a cabo la conexión interna de las interfases correspondientes a la ruta de datos.

3.2.2 Bloqueo de la solicitud de establecimiento

La posibilidad de **bloquear la solicitud de establecimiento** es una característica importante de la tecnología de conmutación de circuitos. Si cualquier otro par de suscriptores llegara a solicitar la red para establecer una conexión que necesite reservar al menos una de las secciones de ruta reservadas para la conexión de A y B, la red negará dicha solicitud. Por ejemplo, si el nodo terminal C envía una solicitud para el establecimiento de una conexión al nodo terminal D, la red bloqueará esta solicitud de establecimiento, pues el único enlace que conecta los switches S2 y S4 está reservado para conectar a los suscriptores A y B.

El bloqueo de la solicitud de establecimiento puede también llevarse a cabo en la sección terminal de la ruta. Por ejemplo, esta situación se presentará si el suscriptor al que se llama está conectado a otro nodo terminal. Cuando esto sucede, la red informa al suscriptor que llama acerca de este desfavorable acontecimiento. Lo anterior es análogo a las redes telefónicas, las cuales responden con señales de corta duración (o con la señal de **línea ocupada**). Algunas redes telefónicas pueden distinguir diferentes situaciones (por ejemplo, **red ocupada** o **suscriptor ocupado**) e informar al suscriptor que llama acerca de lo que está sucediendo mediante el uso de señales a diferentes frecuencias o utilizando diversos tonos.

3.2.3 Ancho de banda garantizado

Suponga que se ha establecido la conexión entre los suscriptores A y B, por lo que solamente ellos cuentan con un circuito caracterizado por un ancho de banda fijo a su disposición. Esto significa que durante todo el tiempo de conexión, los suscriptores deben enviar los datos a la red a una velocidad constante; la red asegurará la entrega de estos datos al suscriptor llamado, sin que se presenten pérdidas y a la misma velocidad. Lo anterior es independiente de si existen otras conexiones en la red durante ese tiempo. El suscriptor no puede transmitir datos a la red a una velocidad que exceda el ancho de banda de la línea. A su vez, la red no puede hacer más lenta la velocidad de transmisión de los datos de usuario.

> La carga de la red influirá sólo en la probabilidad del bloqueo de la solicitud de establecimiento. A medida que haya más conexiones establecidas en la red, la probabilidad de bloqueo de la solicitud de establecimiento será más alta.

Un aspecto positivo es que la red entregue los datos con un retardo pequeño y constante. Los niveles de retardos constantes y bajos en la transmisión de datos, característicos de las redes de conmutación de circuitos, aseguran una alta calidad en la transmisión de datos muy sensibles a los retardos. Esto también se conoce como **tráfico en tiempo real**, siendo la voz y el video algunos ejemplos de este tipo de tráfico.

3.2.4 Multiplexaje

La red simplificada que se describe, *en la que cada enlace físico siempre transmite datos a la misma velocidad,* trabaja de manera ineficaz.

Primero, los usuarios de dichas redes a menudo no obtienen el servicio que esperan. Éstos son usuarios estándar que siempre transmiten información sólo a la velocidad constante disponible. En la actualidad es difícil imaginar a dicho usuario, en especial con la amplia disponibilidad de diferentes tipos de dispositivos terminales, como teléfonos fijos y móviles y computadoras. Por tanto, en general, la velocidad del tráfico de usuarios es diferente del ancho de banda fijo del circuito físico. El ancho de banda puede exceder significativamente o estar por debajo de los requerimientos del usuario. En el primer caso, el usuario no aprovecha al máximo el potencial del circuito; en el segundo, el usuario debe limitar los requerimientos o utilizar varios enlaces físicos.

Segundo, la red emplea de manera ineficaz sus recursos. Evidentemente, la red que se muestra en la figura 3.1 no tiene un número suficiente de enlaces entre los switches. Dicha estructura de red se seleccionó con el fin de ilustrar las razones para bloquear la solicitud de establecimiento. Para reducir la probabilidad de bloqueo a niveles aceptables, es necesario instalar un gran número de enlaces físicos entre los switches. Éste es el método de *mantener el costo.*

Para mejorar la eficacia de las redes de conmutación de circuitos se puede utilizar el multiplexaje, el cual permite transmitir de manera simultánea tráfico proveniente de varias conexiones lógicas utilizando un único enlace físico. El multiplexaje en las redes de conmutación de circuitos tiene características específicas. Por ejemplo, el ancho de banda de cada enlace se divide en **partes iguales**, por lo cual proporciona un número igual de **subcanales**. Observe que para efectos de simplicidad, a menudo los subcanales son llamados simplemente *canales*. En general, los enlaces de comunicaciones que conectan usuarios a las redes soportan un número menor de canales que los enlaces que conectan los switches. En este caso, se reduce la probabilidad de bloqueo. Por ejemplo, el enlace del usuario puede tener 2, 24 o 30 canales; el enlace entre switches puede tener 480 o 1 920 canales. Por el momento, la velocidad más común de un subcanal digital es de 64 Kbps, la cual asegura la transmisión de voz de calidad en un formato digital.

Después de que la red de conmutación de circuitos se complementó con el mecanismo de multiplexaje, su esquema de operación cambió. Las solicitudes de los usuarios para establecer conexiones lógicas ahora sólo reservan uno o varios subcanales del enlace en lugar de todo el canal. Por tanto, las conexiones se establecen a nivel subcanal en lugar de establecerse a nivel enlace. Algunos subcanales deben reservarse para el caso de que el ancho de banda de un solo canal sea insuficiente. Esto permite que el usuario reserve el subcanal (o subcanales) con la velocidad de transmisión de datos más cercana a la que se requiere; además, el multiplexaje facilita construir enlaces más eficaces entre switches. Para reducir la probabilidad de bloqueo se puede utilizar un solo enlace físico con un gran número de subcanales lógicos, en lugar de varios enlaces físicos.

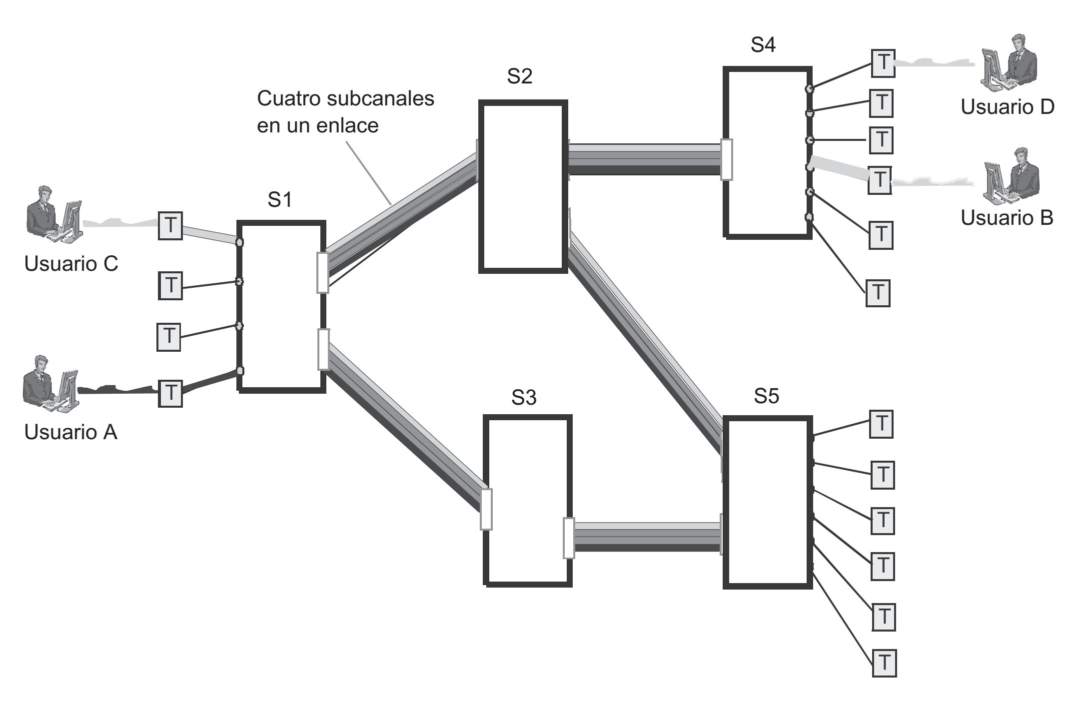


FIGURA 3.3 Conmutación de circuitos con multiplexaje.

La figura 3.3 muestra la red de conmutación de circuitos con multiplexaje. En esta red se hallan establecidas dos conexiones, A-B y C-D, en las cuales la primera utiliza un subcanal en cada enlace de comunicaciones y la segunda dos subcanales en cada enlace. Por tanto, a pesar de la estructura física de la red que se muestra en la figura 3.1, la segunda llamada, C-D, no se bloquea, debido a que los switches soportan la función de multiplexaje.

NOTA *Cuando se utiliza el multiplexaje, la propiedad fundamental de las redes de conmutación de circuitos se conserva y se llama* **canal agregado** *o circuito, que comprende varias secciones de ruta con el ancho de banda empleado previamente. La única diferencia ahora es que el subcanal desempeña el papel de enlace.*

Como es obvio, el uso del multiplexaje complica el procesamiento del tráfico en los switches. En vez de usar procedimientos sencillos y directos de conmutación apropiados a las interfases, ahora es necesario transmitir datos en el canal requerido. Cuando se emplea el multiplexaje por división de tiempo se requiere un gran nivel de sincronización entre los dos flujos de información, mientras que cuando se utiliza el multiplexaje por división de frecuencia, es necesario usar la transformación de frecuencia.

3.2.5 Ineficiencias de la transmisión de tráfico en ráfagas

Existe otra razón por la cual las redes de conmutación de circuitos trabajan a menudo de forma ineficaz y *ésta radica en el principio fundamental de operación de dichas redes, es decir, la reservación de un ancho de banda fijo del circuito durante todo el tiempo de conexión.*

Ya hemos mencionado que el multiplexaje aumenta la eficacia de la red de conmutación de circuitos debido a que ahora los usuarios pueden seleccionar la velocidad de conexión de acuerdo con los requerimientos. Sin embargo, esto solamente tiene que ver con aquellos

usuarios que generan flujos de información a una velocidad constante. ¿Qué hay acerca de los usuarios cuyos flujos de información tienen un comportamiento muy irregular (es decir, que se presenta en intervalos de actividad), tales como el envío de datos en la red seguido de periodos de descanso?

Si usted considera el tráfico de usuarios con más cuidado, encontrará que prácticamente todos los usuarios de las redes de telecomunicaciones se encuentran en esta categoría. Recuerde que los usuarios de las redes telefónicas transmiten información a una velocidad constante. Esta aparente constancia se logra debido a que los flujos irregulares de datos de usuarios son procesados por los dispositivos terminales de la red telefónica: los mismos teléfonos. Por ejemplo, un teléfono digital transmite información a una velocidad constante de 64 Kbps, ya sea que el usuario hable o permanezca en silencio. Como es natural, el teléfono trabajará de manera más eficaz, si éste pudiera *suprimir* las pausas de la conversación y transmitir sólo información útil a la red.

Por último, existe otra categoría de usuarios, cuyos requerimientos en cuanto a la transmisión de información a una velocidad variable son más obvios. Éstos son los usuarios de computadoras.

La actividad de usuario que navega en la web genera tráfico en ráfagas. Cuando se bajan páginas web al usuario de la PC, la velocidad del tráfico aumenta de manera significativa y, después de que ha terminado el proceso de descarga, la velocidad del tráfico desciende prácticamente a cero. Este proceso se repite una y otra vez.

El **coeficiente de pulsación del tráfico** de los usuarios individuales de la red es igual que el cociente del promedio de la intensidad del intercambio de datos entre la máxima intensidad posible. Este coeficiente puede alcanzar un valor de 1:100. Si se implementa la conmutación de circuitos entre la PC del usuario y el servidor, el circuito se caerá durante gran parte de esta sesión. Por otro lado, parte del desempeño de la red se dedicará a este par de nodos terminales. Por tanto, no estará disponible para otros usuarios de la red. La operación de la red durante dichos periodos puede compararse con una escalera eléctrica vacía en una estación del metro, la cual continúa moviéndose indefinidamente, pero no realiza ninguna función útil.

> Las redes de conmutación de circuitos transmiten tráficos de usuario de manera más eficaz cuando el tráfico tiene una intensidad constante a lo largo de toda la sesión y corresponde al ancho de banda de los canales físicos de la red.

Las ventajas y desventajas de cada tecnología de red son relativas. En algunas situaciones, las ventajas son más significativas y las desventajas no tienen consecuencia alguna. Por tanto, la técnica de conmutación de circuitos resulta eficaz cuando es necesario transmitir sólo tráfico telefónico, pues se puede tolerar la imposibilidad de **eliminar** las pausas de las conversaciones. Sin embargo, cuando se transmite tráfico de computadora, el cual es irregular por naturaleza, esta ineficacia se convierte en un aspecto de considerable importancia.

3.3 CONMUTACIÓN DE PAQUETES

> **PALABRAS CLAVE**: paquete, conmutación de paquetes, memoria de entrada, técnica de almacenar y enviar, dispositivo de conmutación, cola de salida, congestión, métodos de envío de paquetes, sin conexión, transmisión de datagramas, datagrama, transmisión orientada a la conexión, circuito virtual, tabla de conmutación, tabla de enrutamiento, tabla de direccionamiento, balanceo de cargas, servicio con el mejor esfuerzo y tiempo de propagación de la señal.

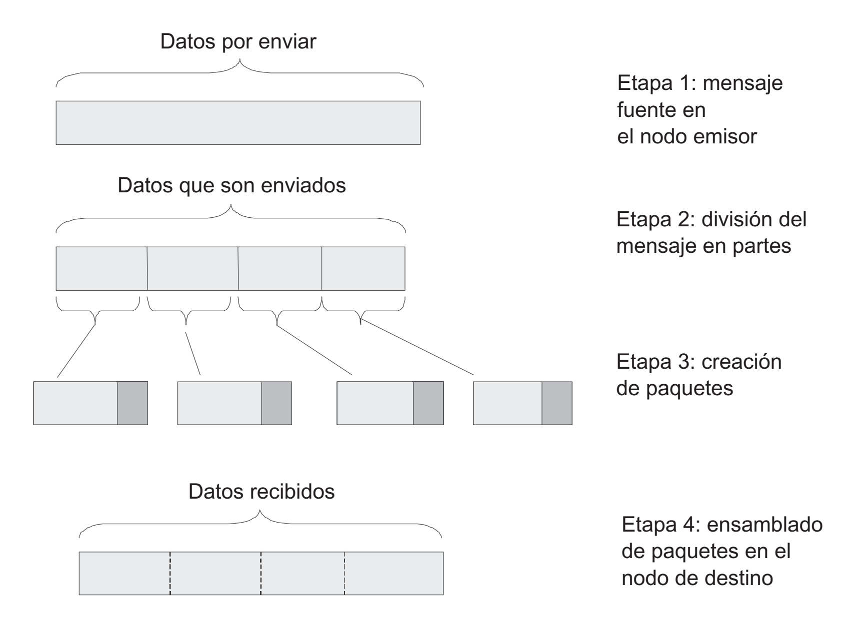


FIGURA 3.4 División de los flujos de datos en paquetes.

La técnica de **conmutación de paquetes** se diseñó especialmente para la transmisión eficaz del tráfico entre computadoras.

Cuando se utiliza la conmutación de paquetes, todos los datos transmitidos por el usuario de la red se dividen en fragmentos relativamente pequeños conocidos con el nombre de **paquetes**, los cuales también se llaman *tramas* o *celdas*, aunque en este contexto la selección del término no tiene importancia. La conmutación de paquetes se lleva a cabo en el nodo transmisor (figura 3.4). Cada paquete cuenta con un encabezado que contiene una dirección, la cual es necesaria para entregar el paquete al nodo de destino. La *presencia de una dirección en cada paquete* representa una de las propiedades más fundamentales de la técnica de conmutación de paquetes, ya que cada paquete *puede*[1] ser procesado por el switch, independientemente de los demás paquetes del flujo de información. Además del encabezado, el paquete cuenta con otro campo auxiliar, el cual está ubicado al final del paquete generalmente y, por tanto, se conoce con el nombre de *remolque*. Este último contiene la suma verificadora, la cual le permite verificar si la información sufrió algún daño durante la transmisión.

Los paquetes se proporcionan a la red *sin la reservación previa de enlaces de comunicación* y a la velocidad a la que los origina la fuente. Dicha velocidad no puede exceder el ancho de banda del enlace de acceso. Se supone que la red de conmutación de paquetes, en contraste con la de conmutación de circuitos, está siempre lista para recibir el paquete de cualquiera de sus nodos terminales.

NOTA *El procedimiento de reservar el ancho de banda también puede utilizarse en una red de conmutación de paquetes; sin embargo, la idea principal de dicha reservación es diferente de la idea de reservación de ancho de banda en redes de conmutación de circuitos. La diferencia es que el ancho de banda del canal en la red de conmutación*

[1] La palabra *puede* en este contexto tiene una especial importancia debido a que en algunas variantes de la tecnología de conmutación de paquetes no se garantiza la independencia total del procesamiento de paquetes (consulte, por ejemplo, la tecnología de los circuitos virtuales).

de paquetes puede ser redistribuido de forma dinámica entre los flujos de información, en función de los requerimientos actuales de cada flujo. Esta posibilidad no puede proporcionarse en las redes de conmutación de circuitos. Los detalles de esta técnica de reservación del ancho de banda se estudiarán con más detalle en el capítulo 7.

3.3.1 Búffers y colas

La red de conmutación de paquetes, como la de conmutación de circuitos, incluye switches conectados mediante enlaces físicos de datos; sin embargo, los switches trabajan de forma diferente en estas redes.

La principal diferencia es que los *switches de paquetes cuentan con memorias internas* para almacenar de manera temporal los paquetes.

En primera instancia, esto se debe a que el switch necesita usar *todas las partes de paquete* para hacer una decisión en cuanto a su direccionamiento. Estas partes incluyen el encabezado, el cual debe contener la dirección de destino, el campo de datos y el remolque que contiene la suma verificadora. El switch verifica la suma verificadora y sólo cuando está seguro de que el paquete de datos no ha sido dañado, comienza a procesar dicho paquete. Esto es, el switch determina el siguiente switch mediante la dirección de destino. Por tanto, *cada* paquete se coloca en la **memoria de entrada** (es decir, de manera secuencial, coloca bit por bit en la memoria asignada al paquete). Teniendo esto en cuenta, es posible decir que las redes de conmutación de paquetes utilizan la **técnica de almacenar y enviar**. Observe que para llevar a cabo esto, es suficiente contar con una memoria igual al tamaño de un solo paquete.

Segundo, se requiere almacenamiento en memoria para coordinar la velocidad de llegada de paquetes y la velocidad de su conmutación. Si la unidad que lleva a cabo la conmutación de paquetes (dispositivo de conmutación) no puede procesar paquetes lo suficientemente rápido, se generarán colas de entrada en las interfases del switch. Para almacenar la cola de entrada, el tamaño de la memoria debe exceder el tamaño de un solo paquete. Existen diferentes métodos para crear un dispositivo de conmutación. El método tradicional se basa en un solo procesador central que atiende a todas las colas de entrada del switch. Este método puede dar como resultado largas colas, ya que el desempeño del procesador se comparte entre varias de ellas. Los métodos modernos para construir los dispositivos de conmutación utilizan multiprocesadores, en los que cada interfase cuenta con su propio procesador integrado para el procesamiento de paquetes; además, existe un procesador central, el cual coordina la operación de los procesadores de las interfases. Mediante el uso de procesadores de interfases se mejora el desempeño del switch y se reducen las colas en las interfases de entrada; sin embargo, dichas colas aún se pueden presentar, ya que el procesador central puede convertirse en un cuello de botella, como sucedió anteriormente. En el capítulo 15 se estudiarán con más detalle los diferentes aspectos de la estructura interna del switch.

Por último, son necesarias las memorias o buffers para coordinar la velocidad de los enlaces conectados a cierto switch de paquetes. Si la velocidad a la que los paquetes se alimentan al switch provenientes de una línea exceden el ancho de banda del enlace al cual estos paquetes necesitan enviarse y esta situación se lleva a cabo en cierto intervalo, con el fin de evitar la pérdida de paquetes es necesario organizar la **cola de salida** en la interfase objetivo (figura 3.5).

De lo anterior se infiere que el paquete reside temporalmente en la memoria del switch, después de lo cual se envía al siguiente switch utilizando la interfase de salida. Dicho método para la transmisión de datos empareja las ráfagas de tráfico en los enlaces troncales entre switches. Esto permite que los canales se utilicen de la manera más eficaz posible permitiendo un incremento en el desempeño de toda la red (figura 3.6).

Switch de paquetes
Cola de entrada
Interfase
Cola de salida
Cola de entrada
Interfase
Cola de salida
Dispositivo de conmutación
Cola de entrada
Interfase
Cola de salida
Cola de entrada
Interfase
Cola de salida

FIGURA 3.5 Colas en el switch de paquetes.

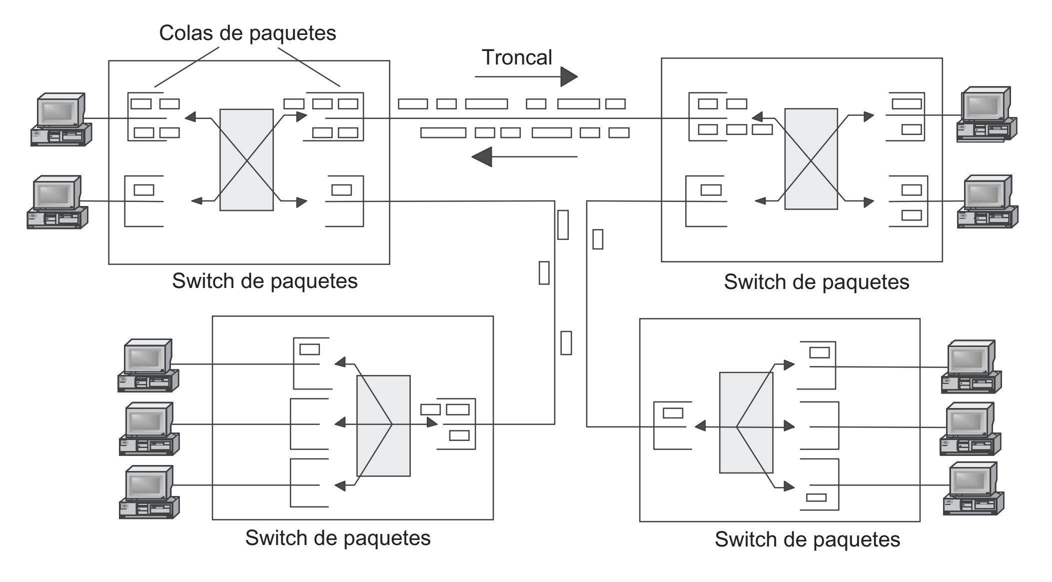


FIGURA 3.6 Emparejamiento de la variación del tráfico en las redes de conmutación de paquetes.

En la red de conmutación de paquetes, las ráfagas de tráfico de los usuarios individuales, de acuerdo con la Ley de los Grandes Números, se distribuyen en el tiempo de tal forma que sus picos, en la mayoría de los casos, no coinciden. Por tanto, los switches estarán cargados constantemente y de manera muy pareja sólo si el número de usuarios atendidos es muy grande. La figura 3.6 muestra que el tráfico que llega de cada uno de los nodos terminales hacia los switches tiene una distribución en el tiempo muy dispareja; sin embargo, los switches

de nivel jerárquico más elevado (aquellos que atienden a las conexiones entre switches de bajo nivel) se cargan de manera más pareja y los enlaces troncales que conectan los switches de niveles superiores tienen una utilización muy cercana al valor máximo. El almacenamiento en memoria empareja las ráfagas de tráfico; por ende, el coeficiente de pulsación en los enlaces troncales es significativamente menor que en los enlaces de acceso del usuario.

Como el tamaño de la memoria en los switches es limitado, los paquetes se pierden a menudo. La sobrecarga temporal de algunos de los segmentos de la red se conoce como **congestión**. Usualmente, esto se lleva a cabo cuando los periodos de pulsación de varios flujos de información coinciden. Como las pérdidas de paquetes representan una propiedad heredada de las redes de conmutación de paquetes se desarrolló un rango específico de mecanismos para compensar este efecto indeseable y garantizar la operación normal de dichas redes. Los métodos que permiten la reducción de la probabilidad de dichas situaciones indeseables se están desarrollando activamente. Se conocen como **calidad de servicio (QoS)** e **ingeniería de tráfico**, los cuales se estudiarán en el capítulo 7.

3.3.2 Métodos de envío de paquetes

La interfase a la cual llegan los paquetes que deben ser enviados se selecciona con base en uno de los tres **métodos de envío de paquetes**:

- **Transmisión no orientada a la conexión**, también conocido como *transmisión de datagramas*. En este caso, la transmisión se lleva a cabo con el establecimiento de una conexión y todos los paquetes transmitidos se *envían de manera independiente* uno del otro aplicando las mismas reglas. El procesamiento de paquetes está determinado solamente por los valores de los parámetros incluidos dentro del paquete y por el estado actual de la red. Por ejemplo, en función de la carga actual, el paquete puede permanecer en la cola por un tiempo más corto o más largo; sin embargo, la red no almacena información acerca de paquetes que ya se hayan transmitido y dicha información no se tiene en cuenta cuando se procesa el paquete siguiente. Esto significa que cada paquete es considerado por la red como una unidad independiente de transmisión de datos conocida como *datagrama*.
- **Transmisión orientada a la conexión.** En este caso, el proceso orientado a la conexión de la transmisión de datos se divide en las llamadas sesiones o conexiones lógicas. La red registra el comienzo y el final de cada conexión lógica. Ahora, el método de procesamiento se determina para todo el *conjunto de paquetes transmitidos como parte de la sesión, en lugar de hacerlo para cada paquete individual.* El proceso de atender cada nuevo paquete entregado depende directamente de la historia previa de la sesión; por ejemplo, si se perdieran varios paquetes anteriores, podría reducirse la velocidad de envío de todos los paquetes subsecuentes.
- **Circuito virtual.** Si la lista de parámetros de conexión incluyera la ruta, todos los paquetes transmitidos como parte de una conexión específica deberán tomar una ruta determinada. Esta constante y predefinida y única ruta que conecta los nodos terminales en la red de conmutación de paquetes se conoce como **circuito virtual** o **canal virtual**.

La clasificación de los métodos de conmutación existentes se presenta en la figura 3.7.

Una misma tecnología de red puede utilizar diferentes métodos de transmisión de datos; por ejemplo, el protocolo de datagramas IP se utiliza para la transmisión de datos entre las diferentes redes que conforman Internet. La entrega confiable de datos entre los nodos terminales de Internet se delega al protocolo TCP orientado a la conexión que establece las conexiones lógicas sin cambiar la ruta. Por último, Internet representa un ejemplo de red

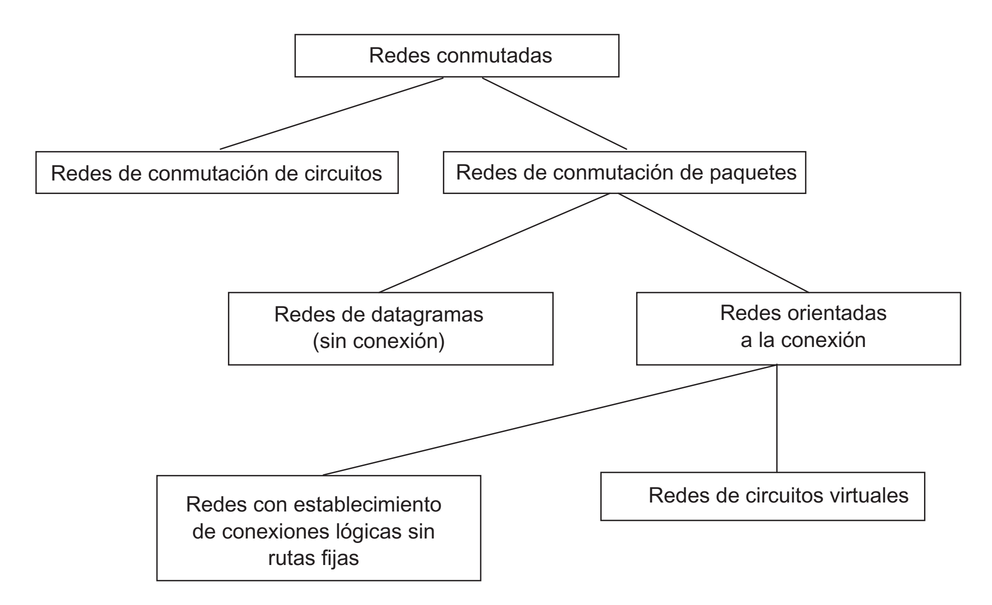


FIGURA 3.7 Taxonomía de las redes conmutadas.

que usa la técnica de circuitos virtuales, ya que incluye varias redes ATM y *Frame Relay* que soportan circuitos virtuales.

3.3.3 Transmisión de datagramas

Como ya se mencionó, el método de transmisión de datagramas se basa en el hecho de que todos los paquetes transmitidos se procesan de manera independiente. La selección de la interfase a la cual es necesario enviar un paquete que llega se lleva a cabo con base en la **dirección destino** especificada en el encabezado del paquete. No se tiene en cuenta el hecho de que ese paquete específico pertenezca a un flujo de información determinado.

La solución al envío de paquetes se basa en una **tabla de conmutación** que contiene el conjunto de direcciones de destino o la información acerca de direcciones que determinan, sin ambigüedades, el siguiente nodo de red en la ruta (ya sea nodo de tránsito o nodo terminal). Recuerde que en las diferentes tecnologías de red se pueden utilizar otros términos para designar la tabla de conmutación: **tabla de enrutamiento**, **tabla de envíos**, etc. Yendo más adelante, para efectos de simplificación, utilizaremos el término *tabla de conmutación* para las tablas de este tipo, las cuales se emplean para transmitir datagramas basadas solamente en las direcciones de los nodos de destino.

Las tablas de conmutación de la red de datagramas deben contener registros para todas las direcciones a las que es posible enviar los paquetes que llegan a las interfases del switch. En general, los paquetes entrantes pueden estar destinados a cualquier nodo de la red. En la práctica, se implementan métodos que ayudan a reducir el número de registros en la tabla de conmutación. Uno de estos métodos es el direccionamiento jerárquico, de acuerdo con el cual la tabla de conmutación puede contener solamente las partes más significativas (las que ocupan las posiciones más hacia la izquierda) de las direcciones que corresponden a un grupo de nodos (subred) más que a nodos individuales. Por tanto, es posible utilizar la analogía de las direcciones de correo, donde los nombres de los países y las ciudades corresponden a las posiciones *más significativas* de las direcciones. Como es natural, los nombres de los países

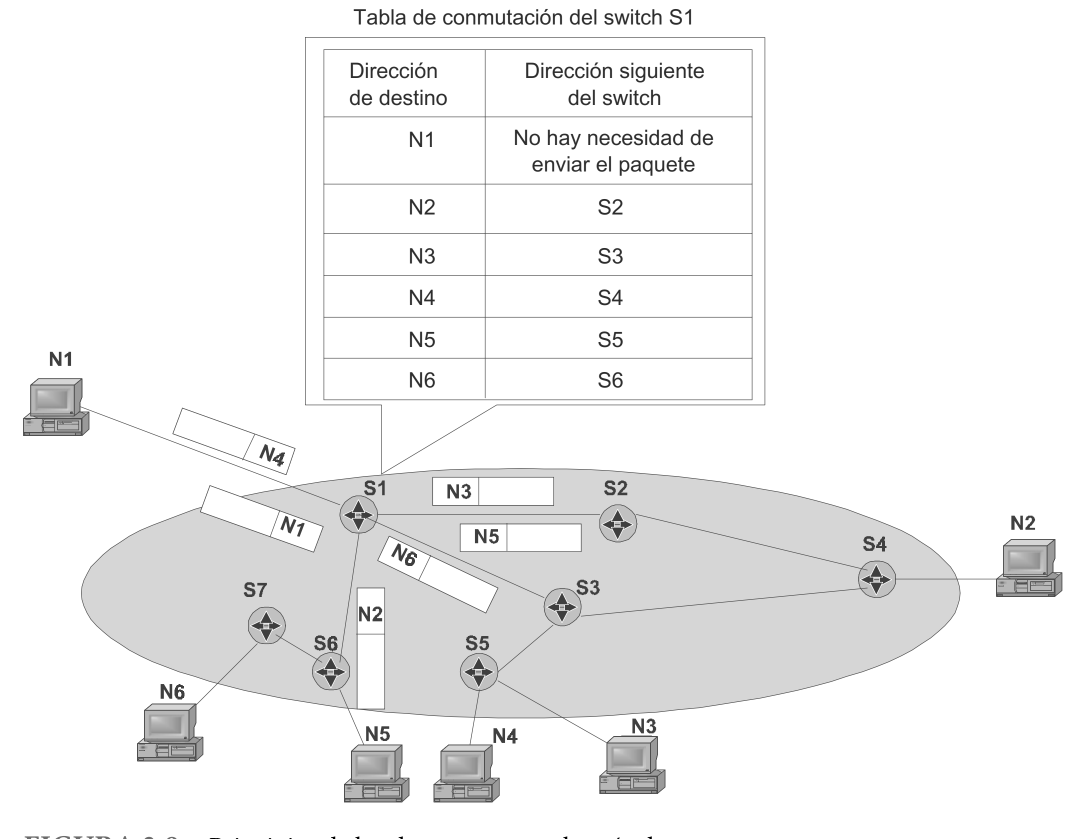


FIGURA 3.8 Principios de los datagramas en el envío de paquetes.

y ciudades son significativamente menos numerosos que los nombres de las calles, números de casa y nombres de las personas. En definitiva son mucho menores en número.

A pesar de usar direccionamiento jerárquico, en algunas redes grandes (por ejemplo, en Internet), los switches aún pueden contar con tablas de conmutación que contengan miles de registros. La figura 3.8 muestra la apariencia de la tabla de conmutación del switch S1 en una red de datagramas.

La tabla de conmutación puede contener varios registros para la misma dirección de destino, especificando distintas direcciones del siguiente switch. Este método se conoce como **balanceo de cargas** y se utiliza para mejorar el desempeño y confiabilidad de la red. En el ejemplo que se muestra en la figura 3.8, los paquetes que llegan al switch S1, con destino al nodo N2, están distribuidos entre los switches siguientes S2 y S3 con el fin de balancear la red. Esto reduce la carga de trabajo de los switches S2 y S3 y, en consecuencia, también reduce las colas y acelera la entrega. Alguna **confusión** en las rutas de los paquetes con la misma dirección de destino representa una consecuencia directa del principio de procesamiento independiente de paquetes, el cual es inherente al método de datagramas. Los paquetes que tienen la misma dirección de destino pueden entregarse a esa dirección vía rutas distintas debido al cambio en el estado de la red, tales como la falla de algunos switches de tránsito.

El método de entrega de datagramas es rápido, pues no se requiere hacer preparativos antes de que se lleve a cabo la transmisión de datos; sin embargo, cuando se aplica este método, es difícil rastrear la entrega de paquetes al nodo de destino. Por tanto, este método no garantiza la entrega de paquetes, aunque una red haga su mejor esfuerzo en entregarlo a su destino correcto. Dicho servicio se conoce como **servicio con el mejor esfuerzo**.

3.3.4 Conexión lógica

La transmisión orientada a la conexión se basa en el conocimiento de los antecedentes del intercambio de paquetes (es decir, los valores actuales de la conexión). Permite usar un método más racional en el procesamiento de cada paquete nuevo que llega. Los parámetros de conexión pueden utilizarse para diferentes propósitos; por ejemplo, se puede usar la numeración de paquetes y rastrear los números de los paquetes enviados y recibidos para mejorar la confiabilidad de la transmisión. Lo anterior facilita eliminar paquetes duplicados, ordenar los paquetes recibidos y repetir los envíos de paquetes perdidos dentro del contexto de una conexión específica. Entre los parámetros de una conexión segura deberá estar la información acerca del método de encriptado.

Los parámetros de conexión pueden ser constantes durante todo el tiempo de conexión (por ejemplo, el tamaño máximo de paquetes) o variable, reflejando de manera dinámica el estado actual de la conexión (por ejemplo, los números de paquetes secuenciales mencionados anteriormente). Cuando el emisor y el receptor establecen una nueva conexión, primero negocian respecto a los parámetros iniciales del procedimiento de intercambio y solamente después del comienzo de la transmisión de datos.

Los protocolos orientados a la conexión garantizan una transmisión más confiable; sin embargo, requieren más tiempo para la transmisión de datos e imponen cargas de procesamiento más altas en los nodos terminales (figura 3.9).

Cuando se utiliza la transmisión orientada a la conexión, el nodo de origen envía al nodo de destino un paquete de servicio con un formato especial que contiene una solicitud para establecer una conexión (figura 3.9*b*). Si el nodo de destino está de acuerdo en establecer la conexión, éste le responde al nodo de origen con otro paquete de servicio, conformando el establecimiento de la conexión y sugiriendo que se utilicen algunos parámetros dentro de esta

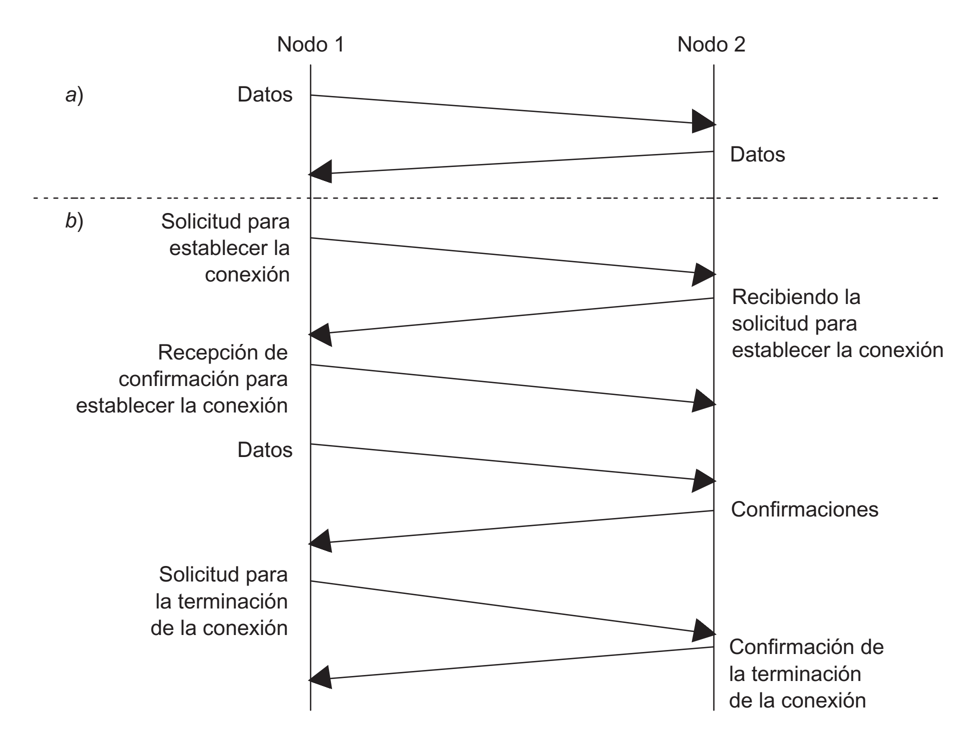


FIGURA 3.9 Transmisión sin establecer una conexión *a*) y estableciendo una conexión *b*).

conexión lógica. Entre dichos parámetros se incluye un identificador de la conexión, el valor máximo de la longitud del campo de datos del paquete y el número máximo de paquetes que pueden enviarse sin recibir confirmación. El nodo que inicia la conexión puede terminar el proceso del establecimiento enviando un tercer paquete de servicio con información de que los parámetros sugeridos son aceptables. Después de esto, la conexión lógica se considera establecida. Las conexiones lógicas pueden estar diseñadas para la transmisión de datos unidireccional (desde el iniciador de la conexión) y para el intercambio bidireccional de datos. Una vez transmitidos algunos grupos de datos lógicamente completos (por ejemplo, un archivo específico), el nodo emisor inicia el procedimiento de terminación de la conexión enviando un paquete de servicio apropiado.

Observe que en contraste con la transmisión de datagramas que soporta solamente un tipo de paquete, la transmisión orientada a la conexión debe soportar al menos dos tipos de paquetes. Éstos son los paquetes de servicio que se utilizan para establecer (o terminar) conexiones y los paquetes de información que se emplean para transmitir los datos del usuario.

3.3.5 Circuitos virtuales

El mecanismo de **circuitos virtuales (canales virtuales)** crea rutas fijas estables para la transmisión de tráfico en redes de conmutación de paquetes. Todos los paquetes relacionados con la misma conexión lógica siguen la misma ruta: circuito virtual. Las redes basadas en las tecnologías X.25, *Frame Relay* y ATM utilizan este mecanismo.

Los circuitos virtuales vislumbran la existencia de flujos de datos en la red. Para identificar un flujo de datos en el tráfico agregado, cada paquete de dicho flujo está especialmente marcado. En las redes de este tipo, la transmisión de datos implica el procedimiento preliminar de establecer de una conexión lógica conocida como circuito virtual. De manera similar al procedimiento de establecer conexiones lógicas, la creación de circuitos virtuales comienza con una solicitud para establecer una conexión enviada por el nodo origen. Las solicitudes de conexión representan paquetes de servicio con un formato especial, también conocido como **paquetes de configuración**. El paquete de configuración debe contener la dirección de destino y la etiqueta del flujo para el que se creó este circuito virtual. El paquete de servicio se transfiere por medio de la red y registra la información de control acerca de todos los switches ubicados a lo largo de la ruta entre el emisor y el receptor. Con base en esta información, se forma el registro de la tabla de conmutación, especificando cómo debe atender el switch el paquete que tiene esta etiqueta. Un circuito virtual creado en dicha forma se identifica con la misma etiqueta.[2]

Después de que se ha creado el circuito virtual, la red puede comenzar a transmitir el flujo de datos a través de ésta. En todos los paquetes que transportan datos de usuario, la dirección de destino no se especifica. En lugar de la dirección de destino, los paquetes de información contienen solamente la etiqueta del circuito virtual. Cuando el paquete llega a la interfase de entrada del switch, éste lee el valor de la etiqueta del encabezado del paquete que llegó y consulta su tabla de conmutación. Posteriormente, encuentra el registro que especifica el puerto de salida por el cual deberá enviarse este paquete.

[2] En las diferentes tecnologías, esta etiqueta tiene nombres distintos: número de circuito lógico (LCN) en X.25, identificador de conexión al enlace de datos (DLCI) en *Frame Relay* e identificador de circuito virtual (VCI) en ATM.

Las tablas de conmutación de las redes que utilizan el mecanismo de circuito virtual son diferentes de las tablas de conmutación de las redes de datagramas. En contraste con las redes que usan el algoritmo de direccionamiento de datagramas, en el cual las tablas de conmutación contienen información acerca de todas las direcciones de destino posibles, las tablas de conmutación de las redes de circuito virtual contienen registros acerca solamente de circuitos virtuales que pasan a través de este switch. En general, en una red de gran tamaño, el número de circuitos virtuales que pasan a través de un nodo específico es significativamente menor que el número total de nodos. Por tanto, el tamaño de la tabla de conmutación es significativamente más pequeño. En consecuencia, la consulta del registro requerido en esta tabla toma menos tiempo y no requiere una significativa cantidad de procesamiento por parte del switch. Debido a esto, la etiqueta es mucho más corta que la dirección del nodo destino, lo cual reduce la cantidad de información innecesaria del paquete, ya que ahora contiene un ID corto del flujo de datos en lugar de una larga dirección de destino.

NOTA *Es necesario hacer hincapié en que el uso de las técnicas de circuitos virtuales en una red no la hace una red de conmutación de circuitos. Aunque éstas utilizan el procedimiento de establecimiento de circuitos, dicho circuito es virtual. Transmite paquetes individuales en lugar de flujos de información que viajan a velocidad constante, como las redes de conmutación de circuitos.*

La figura 3.10 muestra un fragmento de la red en el que se han creado dos circuitos virtuales. El primero comienza en el nodo terminal con la dirección N1 y termina en el nodo con la dirección N2, pasando a través de los switches de tránsito S1, S3 y S4. El segundo circuito garantiza el envío de datos a través de la ruta N3-S5-S7-S4-N2. Por tanto, entre dos nodos terminales pueden existir varios circuitos virtuales.

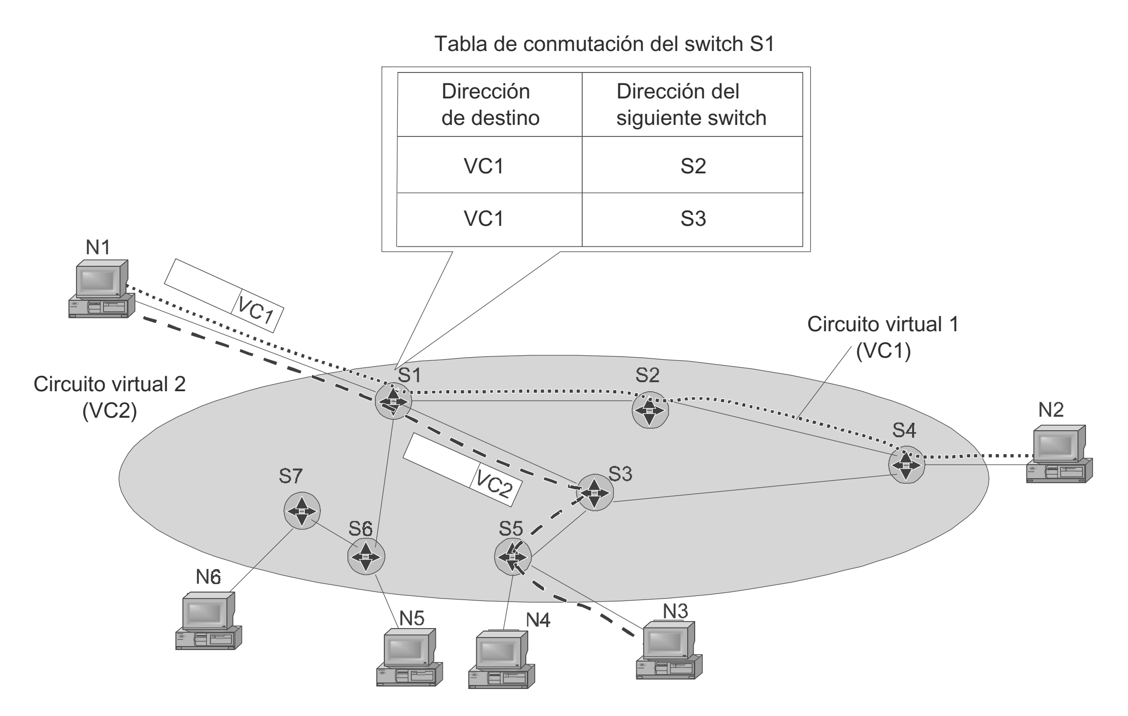


FIGURA 3.10 Principio de operación de los circuitos virtuales.

3.3.6 Redes de conmutación de circuitos en oposición a redes de conmutación de paquetes

Antes de llevar a cabo la comparación técnica de las redes de conmutación de paquetes y de conmutación de circuitos, resulta útil considerar su comparación informal con base en una analogía con el tráfico motorizado.

Analogía de transporte de las redes de conmutación de circuitos y de paquetes

Cuando utilizamos esta analogía, los autos corresponden a los paquetes de datos y los caminos y carreteras corresponden a los enlaces de comunicaciones. De manera similar que los paquetes de datos, los autos se mueven de manera independiente, los cuales comparten el camino y se obstaculizan unos con otros. Si el tráfico es demasiado intenso y no corresponde al espacio disponible en el camino, se puede presentar una congestión. Como resultado de esto, los autos se retrasan en los embotellamientos de tránsito, lo cual corresponde a las colas de paquetes que se presentan en los switches.

La conmutación de los flujos de autos se lleva a cabo en los caminos cruzados y en la intersección de calles, donde el conductor de cada auto selecciona una dirección adecuada para llegar a su destino. Como es natural, el papel de una intersección de caminos comparada con el switch de paquetes es pasiva. Su participación activa en el procesamiento de tráfico es notable solamente en intersecciones controladas por semáforos, donde la luz del semáforo define el turno que cada flujo de autos tiene para cruzar la intersección. Como es natural, si un agente de tránsito lleva a cabo esta función, el papel que éste desempeñaría sería más activo debido a que podría escoger un determinado auto de todo el flujo y permitir que su conductor realizara la maniobra.

La misma analogía puede utilizarse con el transporte citadino para comparar las redes de conmutación de paquetes y las de conmutación de circuitos.

A veces deben garantizarse condiciones específicas para mover una fila de autos. Por ejemplo, suponga que una larga fila de autobuses lleva a unos niños a un campo de verano. Esta fila se mueve a lo largo de la carretera utilizando múltiples carriles. Para garantizar el movimiento sin obstáculos es necesario seleccionar su ruta con antelación. Después, a lo largo de toda la ruta predefinida que cruza varias intersecciones, se asigna un carril por separado a esta fila. El agente de tránsito reserva este carril para los autobuses con niños, garantizando que no lo usarán otros autos. Esta reservación se cancela sólo después de que la fila haya llegado a su destino.

Durante el viaje, todos los camiones se mueven a la misma velocidad en intervalos aproximadamente iguales con el fin de evitar la creación de obstáculos entre ellos. Obviamente, se generan condiciones privilegiadas para dicha fila; sin embargo, en este caso, los autos dejan de moverse en forma independiente. Por el contrario, siguen en el flujo del cual es imposible salir. La carretera en estas condiciones tiene un uso ineficaz debido a que el carril no se emplea por mucho tiempo, de modo similar al ineficiente uso del ancho de banda en las redes de conmutación de circuitos.

Comparación cuantitativa de los retardos

Ahora, a partir de la analogía del transporte, regresemos al tráfico de la red. Imagine que un usuario necesita transmitir tráfico en ráfagas, el cual está formado por periodos de actividad y pausas. Suponga también que el usuario puede seleccionar si transmitir este tráfico a través de una red de conmutación de circuitos o una de conmutación de paquetes. En ambos casos,

el ancho de banda del enlace de comunicaciones es el mismo. Una red de conmutación de circuitos sería la opción más eficaz para este usuario, en cuanto al requerimiento del tiempo; en una red de conmutación de circuitos, el usuario tiene un circuito de comunicaciones reservado a su exclusiva disposición. Si se aplica este método, todos los datos deberán entregarse en su destino sin retardo. Durante periodos significativos del tiempo de conexión, el circuito de comunicaciones reservado se utilizaría de manera ineficiente (durante las pausas); sin embargo, esto es de muy poca o nula importancia debido a que el objetivo principal del usuario es resolver los problemas tan pronto como le sea posible.

Cuando el usuario opte por usar la red de conmutación de paquetes, el proceso de transmisión de datos será más lento, ya que los paquetes enviados por el usuario hacia el destino tienen mayor probabilidad de sufrir retardos en las colas más de una vez conforme éstos recorren la ruta. Las redes de conmutación de paquetes reducen la velocidad de transmisión de datos de los usuarios individuales, ya que los paquetes del usuario comparten todos los recursos de la red con los paquetes enviados por los demás usuarios.

Considere las causas que originan los retardos en la transmisión de datos en ambos tipos de redes con más detalle. Suponga que el nodo terminal N1 envía un mensaje al nodo terminal N2. A lo largo de la ruta por la que se transmiten los datos, existen dos switches.

En una red de conmutación de circuitos, la transmisión de datos comienza a la velocidad estándar del circuito, después de un retardo inicial causado por la necesidad de establecer el circuito (figura 3.11). El tiempo (*T*) requerido para entregar los datos al nodo destino es igual que la suma del tiempo de propagación de la señal (t_{prg}) y del tiempo de transmisión del mensaje (t_{trns}). Observe que la presencia de switches no ejerce alguna influencia en el tiempo total que se requiere para la transmisión de datos.

NOTA *Observe que el tiempo de transmisión del mensaje coincide exactamente con el tiempo requerido para recibir el mensaje proveniente del canal hacia la memoria del nodo de destino. En este caso se le llama tiempo de almacenamiento.*

- El **tiempo de propagación de la señal** depende de la distancia entre el origen y el destino (*L*) y de la velocidad de la propagación de las ondas electromagnéticas en el medio físico (*S*), la cual varía dentro del rango de $0.6v_{luz}$ a $0.9v_{luz}$, donde v_{luz} es la velocidad de la propagación de la luz en el vacío. Por tanto, $t_{prg} = L/S$.

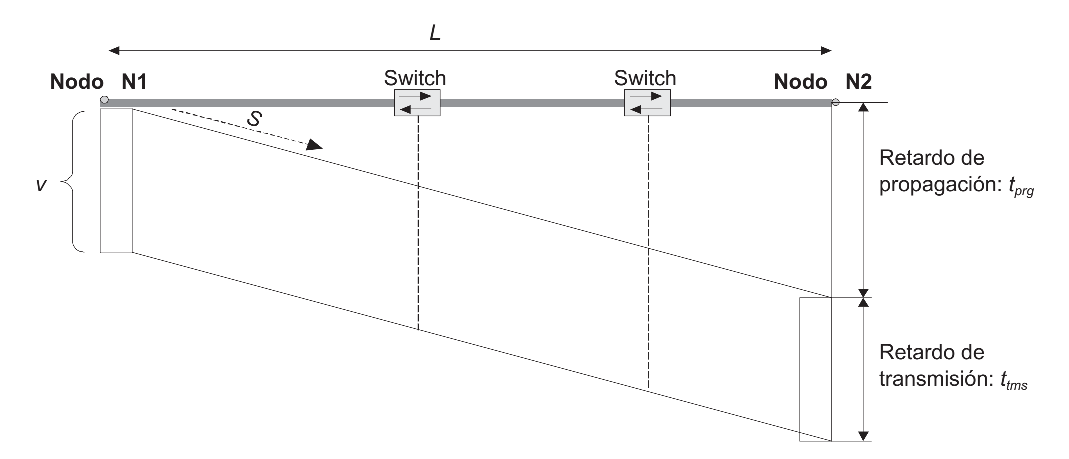


FIGURA 3.11 Diagrama de tiempos de la transmisión de mensajes en una red de conmutación de circuitos.

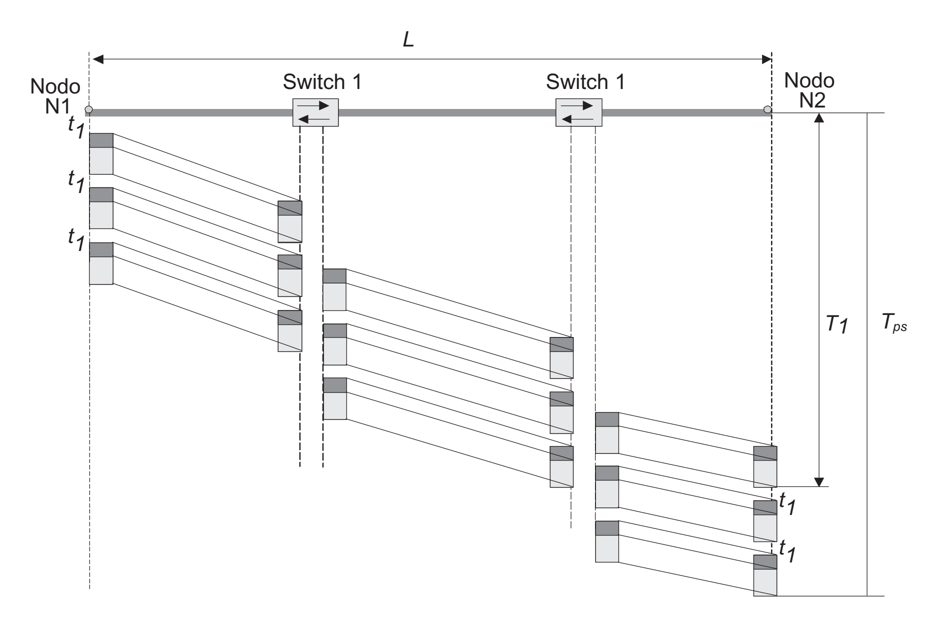


FIGURA 3.12 Diagrama de tiempos de la transmisión de un mensaje dividido en paquetes en una red de conmutación de paquetes.

- El **tiempo de transmisión del mensaje** es igual que el cociente del volumen del mensaje (V) en bits y el ancho de banda del circuito (C) en bits por segundo: $t_{trns} = V/C$.

En las redes de conmutación de paquetes, el procedimiento de la transmisión de datos no requiere establecer de manera obligada la conexión.

Suponga que la red de conmutación de paquetes (figura 3.12) transmite un mensaje del mismo tamaño (V) que el mensaje en el ejemplo anterior (consulte la figura 3.11); sin embargo, en este caso el mensaje se divide en paquetes y cada uno cuenta con un encabezado. Dichos paquetes se transmiten del nodo N1 al N2, entre los que existen dos switches. Los paquetes de cada switch se muestran dos veces: una vez en el momento en que los paquetes llegan a la interfase de entrada y luego conforme el paquete se transmite hacia la red desde la interfase de salida. Es evidente que cada switch retarda por determinado tiempo la transmisión de paquetes. El tiempo designado como T_{ps} significa el tiempo que se requiere para la entrega de datos a su destino en la red de conmutación de paquetes, mientras que T_1 es el tiempo que se necesita para transmitir un solo paquete (el primero) a través de la red.

Cuando se comparan los diagramas de tiempo observe los dos hechos siguientes:

- El tiempo de propagación de la señal t_{prg} tiene el **mismo valor** en ambas redes, siempre y cuando la distancia de transmisión y el medio físico sea el mismo.
- Teniendo en cuenta que los valores del ancho de banda del enlace de ambas redes son el mismo, se puede llegar a la conclusión de que el tiempo de transmisión del mensaje —t_{trns}— tendrá también el **mismo valor**.

Sin embargo, el proceso de dividir el mensaje que se transmite en paquetes y la transmisión de dichos paquetes a través de la red de conmutación de paquetes tiene una influencia significativa en el tiempo que se requiere para entregar el mensaje a su destino. El tiempo de entrega aumenta como resultado de los retardos adicionales.

Rastree la ruta de un solo paquete, asígnele el número 1, tome nota de los componentes que forman el tiempo total requerido para transmitirlo hacia el nodo destino y luego determine qué componentes son específicos para las redes de conmutación de paquetes (figura 3.13).

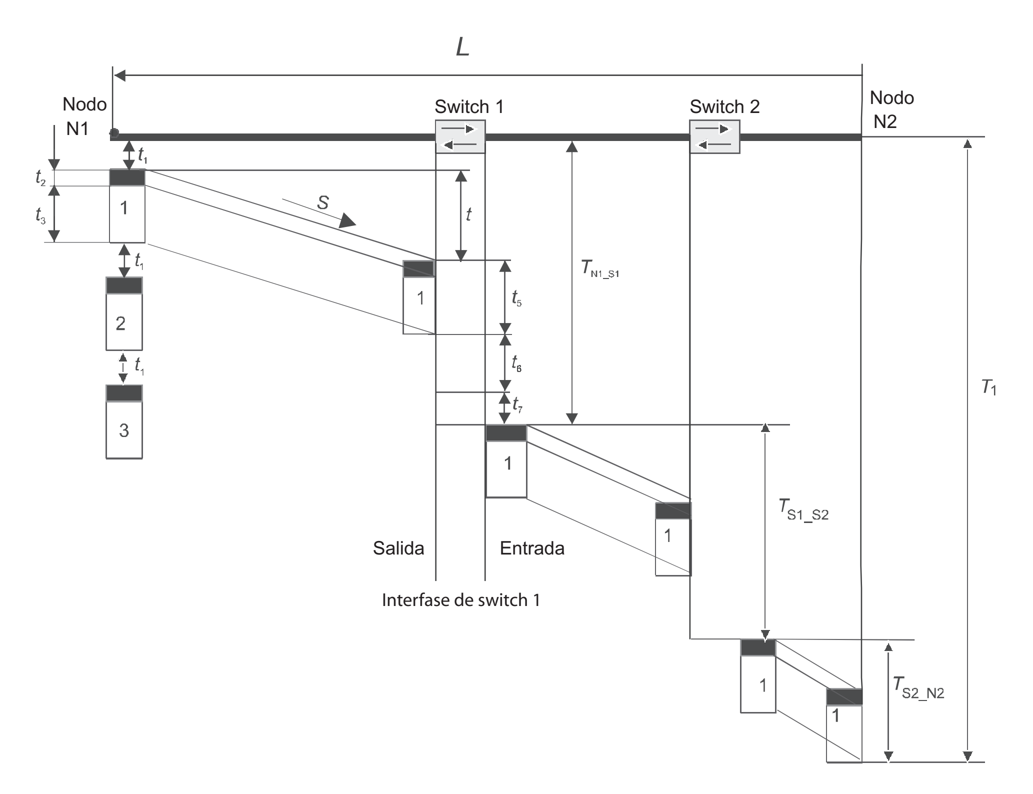


FIGURA 3.13 Diagrama de tiempos para la transmisión de un solo paquete a través de la red de conmutación de paquetes.

El tiempo que se requiere para transmitir un solo paquete del nodo N1 al *switch 1* puede representarse como la suma de los componentes que siguen:

- En el nodo de origen, el retardo en tiempo consta de los componentes que se listan en seguida:
  - t_1: tiempo requerido para formar el paquete; también se le conoce como *tiempo de paquetización*. El valor de este retardo depende de los diferentes parámetros del software y hardware del nodo emisor y no depende de los parámetros de la red.
  - t_2: tiempo requerido para el envío del encabezado del paquete al canal.
  - t_3: tiempo requerido para enviar el campo de datos del paquete al canal.
- Segundo, se necesita tiempo adicional para la propagación de señales a través de los enlaces de comunicación. El tiempo requerido para que la señal que representa un bit de información se propague del nodo N1 al switch 1 se expresa como t_4.
- Tercero, se consume determinado tiempo adicional en el switch de tránsito, el cual puede representarse como la suma de los componentes que siguen:
  - t_5: tiempo requerido para recibir el paquete con su encabezado en la memoria de entrada del switch. Como lo mencionamos anteriormente, este tiempo es igual que ($t_2 + t_3$): el tiempo requerido para enviar el paquete con su encabezado desde el nodo de origen hasta el enlace.
  - t_6: tiempo que pasa el paquete en la cola. Este valor puede variar ampliamente y no se conoce su valor con antelación, ya que depende de la carga actual de la red.

- t_7: tiempo requerido para enviar el paquete al puerto de salida. Este valor es constante para el modelo del switch en particular y generalmente es muy pequeño. Puede variar desde varios microsegundos hasta milisegundos.

El tiempo requerido para enviar el paquete del nodo N1 a la interfase de salida del switch 1 se expresa como $T_{N1\text{-}S1}$. Este tiempo es la suma de los componentes siguientes:

$$T_{N1\text{-}S1} = t_1 + t_4 + t_5 + t_6 + t_7.$$

Observe que t_2 y t_3 no están en la lista de componentes. De la figura 3.13 es evidente que la transmisión de bits del transmisor hacia el enlace coincide en tiempo con la transmisión en bits a través del enlace de comunicaciones.

Los tiempos requeridos para transmitir el paquete a través de las dos secciones de ruta que quedan se designan, respectivamente, como $T_{S1\text{-}S2}$ y $T_{S2\text{-}N2}$. Ambos tienen la misma estructura que $T_{N1\text{-}S1}$, excepto que no incluyen el componente de tiempo t_1 requerido para formar el paquete y, adicionalmente, $T_{S2\text{-}N2}$ no incluye el tiempo de conmutación, ya que la sección termina con el nodo terminal. Por tanto, el tiempo total requerido para transmitir un solo paquete a través de la red puede expresarse como sigue: $T_1 = T_{N1\text{-}S1} + T_{S1\text{-}S2} + T_{S2\text{-}N2}$.

Entonces, ¿cuánto tiempo tomará transmitir varios paquetes?, ¿cuál es la suma de los tiempos requeridos para transmitir cada paquete? ¡No! Recuerde que la red de conmutación de paquetes opera como una tubería (figura 3.12). El procesamiento de paquetes se presenta en varias etapas y todos los dispositivos de la red llevan a cabo estas operaciones en paralelo. Por tanto, el tiempo requerido para transmitir dicho mensaje será considerablemente menor que el tiempo requerido para transmitir cada paquete de manera individual. Es difícil calcular este tiempo con precisión debido a la incertidumbre del estado de la red en cualquier instancia de tiempo. En consecuencia, el tiempo que deberán esperar los paquetes en las colas de los switches también es incierto. Sin embargo, con base en el supuesto de que los paquetes esperan en colas durante aproximadamente espacios iguales, es posible evaluar el tiempo total T_{PS} requerido para transmitir el mensaje que consiste en n paquetes como sigue:

$$T_{PS} = (T_1 + (N - 1)\ (t_1 + t_5).$$

EJEMPLO

Utilice el ejemplo que se muestra en la figura 3.13 para realizar un estimado grosso modo *del retardo en la transmisión de datos en las redes de conmutación de paquetes en comparación con las redes de conmutación de circuitos. Suponga que el mensaje de texto que debe transmitirse en ambos tipos de redes sea de alrededor de 200 000 bytes. La distancia entre el emisor y el receptor es de 5 000 km. El ancho de banda de los enlaces de comunicaciones es de 2 Mbps.*

El tiempo para la transmisión de datos en la red de conmutación de circuitos está formado por los componentes que siguen:

- *El tiempo de propagación de la señal que para la distancia de 5 000 km puede calcularse de forma aproximada como de 25 mseg.*
- *El tiempo de transmisión del mensaje, el cual para las condiciones dadas (ancho de banda igual que 2 Mbps y tamaño del mensaje igual que 200 000 bytes) es aproximadamente de 800 mseg.*

Esto significa que el tiempo total requerido para transmitir este mensaje es de 825 mseg. Ahora evalúe el tiempo extra que será necesario para transmitir el mismo mensaje a través de una red de conmutación de paquetes. Suponga que la ruta del emisor al receptor incluye 10 switches; además, asuma que la red no trabaja con toda la carga; por tanto, no hay colas en los switches. El mensaje de origen se divide en 200 paquetes de 1 000 bytes cada uno.

Si asumimos que el intervalo entre cada paquete enviado es igual que 1 mseg, los retardos adicionales provocados por estos intervalos serán de alrededor de 200 mseg. Por tanto, un retardo adicional para dividir el mensaje en paquetes igual que 280 mseg surgirá en el nodo de origen. Suponga que la información de relleno contenida en los encabezados de los paquetes forma 10% del tamaño total del mensaje. En consecuencia, el retardo adicional relacionado con la transmisión de los encabezados de paquetes forma 10% del tiempo total de la transmisión del mensaje (es decir, 80 mseg). A medida que los paquetes pasan a través de cada switch, se introduce un retardo de memoria. Para una longitud de paquete de 1 000 bytes y un ancho de banda del enlace de comunicaciones igual que 2 Mbps, este valor será de 4.4 mseg por cada switch; además, existe un retardo de conmutación. En este ejemplo, suponga que la conmutación toma alrededor de 2 mseg. En consecuencia, el paquete que ha circulado por 10 switches llega con un retardo total igual que 64 mseg debido al almacenamiento y la conmutación. Como resultado de esto, la red de conmutación de paquetes genera un retardo adicional de 344 mseg.

Con la transmisión de datos en la red de conmutación de circuitos de 825 mseg, este retardo adicional puede considerarse insignificante. Aunque los cálculos proporcionados aquí son grosso modo*, ayudan a clarificar las razones por las que, para los usuarios individuales, el proceso de la transmisión de datos en las redes de conmutación de paquetes es a menudo significativamente más lento que el mismo proceso en las redes de conmutación de circuitos.*

¿A qué conclusión puede llegarse con base en este cálculo?, ¿son las redes de conmutación de circuitos más eficaces que las de conmutación de paquetes?

Cuando se consideran las redes en general, no es conveniente utilizar la velocidad de transmisión del tráfico de un usuario individual como un criterio de eficiencia. En lugar de eso, tiene sentido utilizar un criterio más integral como la *cantidad total de datos transmitidos por la red por unidad de tiempo.* De acuerdo con este criterio, la eficiencia de la red de conmutación de paquetes probará ser significativamente mejor que la eficiencia de la red de conmutación de circuitos con el mismo ancho de banda de los enlaces de comunicaciones. Este resultado fue demostrado en la década de 1960 tanto experimental como analíticamente (con base en la teoría de colas).

EJEMPLO *Compare la eficiencia de las redes de conmutación de circuitos y de paquetes utilizando el ejemplo que se muestra en la figura 3.14. Dos switches están conectados mediante un enlace con un ancho de banda de 100 Mbps. Los usuarios están conectados a la red a través de los enlaces de acceso caracterizados por un ancho de banda de 10 Mbps. Para simplificar este argumento, suponga que todos los usuarios generan el mismo tráfico en ráfagas a una velocidad promedio de 1 Mbps. Al mismo tiempo, por periodos muy cortos, la velocidad de esta carga ofrecida se incrementa al ancho de banda máximo del enlace de acceso (es decir, a 10 Mbps). Dichos periodos nunca duran más de un segundo. Para simplificar más la comparación, suponga que todos los usuarios conectados al switch S1 necesitan transmitir constantemente información a los usuarios conectados al switch S2.*

Suponga que la red que se muestra en la figura 3.14 es una red de conmutación de circuitos. Como los picos del tráfico del usuario alcanzan los 10 Mbps, cada usuario debe establecer una conexión caracterizada por el ancho de banda de 10 Mbps.

Por tanto, sólo 10 usuarios podrán transmitir datos de manera simultánea a través de la red. La velocidad promedio total de información transmitida a través de esta red será igual que 10 Mbps; esto es, 10 usuarios transmiten datos a una velocidad promedio de 1 Mbps. En consecuencia, aunque el enlace de comunicaciones entre los switches tiene un ancho de banda igual que 100 Mbps, solamente 10% de este ancho de banda se utiliza en realidad.

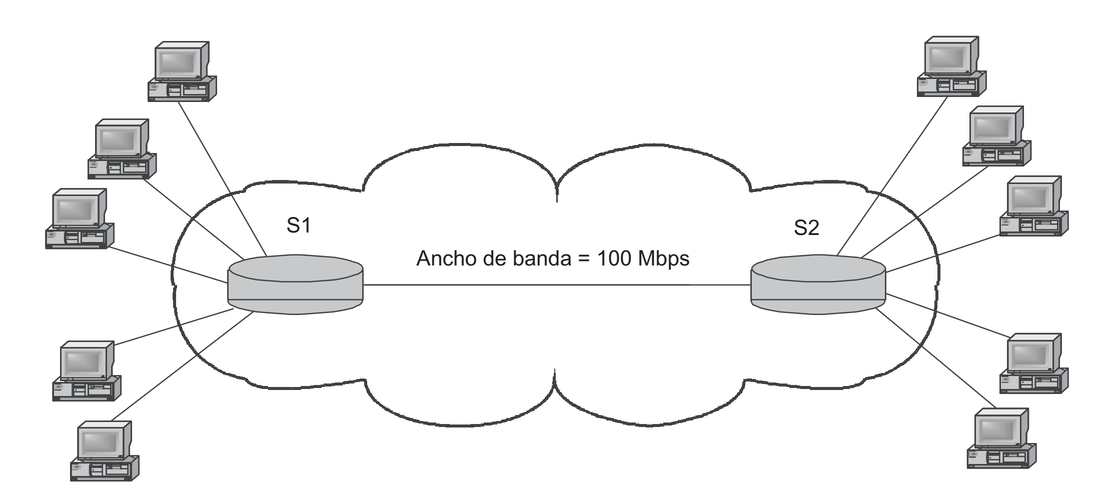


FIGURA 3.14 Comparación entre la red de conmutación de paquetes y la red de conmutación de circuitos.

Ahora considere una situación en la que la misma red trabaja con base en la conmutación de paquetes. Para una velocidad de datos promedio de tráfico de usuario igual que 1 Mbps, la red es capaz de transmitir de manera simultánea hasta 100/1 = 100 flujos de información de datos de usuario, empleando totalmente el ancho de banda del enlace que conecta los dos switches; sin embargo, esto es válido solamente cuando los tamaños de las memorias de los switches son suficientes para almacenar los paquetes durante el tiempo de congestión, cuando la velocidad total de los flujos de datos excede 100 Mbps. Trate de evaluar grosso modo *el tamaño de memoria requerido del switch S1. Sabemos que cada flujo transmite a la máxima velocidad posible de 10 Mbps (limitado por el ancho de banda del enlace de acceso) por intervalos de no más de 1 segundo. Durante este tiempo, el flujo transmitirá 10 Mbits de datos de usuario y en el escenario de peor caso de congestión de la red, 100 de dichos flujos llegarán a las interfases de entrada del switch S1. La cantidad de datos total proporcionada al switch S1 durante este tiempo será de 1 000 Mbits. Durante el mismo periodo, el switch S1 podrá transmitir solamente 100 Mbps en el enlace de salida. En consecuencia, para garantizar que no se pierda ningún paquete durante la congestión de la red, es necesario asegurar que el switch S1 cuente con memorias de entrada no menores que 1 000 – 100 = 900 Mbits o aproximadamente 100 MB. Este tamaño de memoria es muy grande para la industria electrónica actual. Con mucha frecuencia, los switches tienen tamaños de memoria más pequeños, entre 1 y 10 MB; sin embargo, no olvide que es poca la probabilidad de que coincidan los periodos de carga pico para todos los flujos. Por tanto, aun si el switch tiene una cantidad más pequeña de memoria de almacenamiento que la requerida incluso en la situación más difícil, en la mayoría de los casos el switch manejará la carga ofrecida, garantizando una mejor calidad de servicio para cada flujo.*

Aquí, uno puede hacer una analogía con los sistemas operativos multitareas. En dichos sistemas, cada programa específico o tarea corre en más tiempo que en un sistema monotarea, en el cual todo el tiempo de procesamiento está asignado al programa hasta que se termina su ejecución. No obstante, el número total de programas ejecutados por unidad de tiempo en un sistema multitarea es significativamente mayor. De manera similar a un sistema operativo monotarea, en el que el procesador o los dispositivos periféricos están sin hacer nada de vez

en cuando, las redes de conmutación de circuitos no suelen utilizar una parte significativa del ancho de banda del canal reservado cuando transmiten tráfico en ráfagas.

La utilización indeterminada de la red de conmutación de paquetes es el pago por su eficiencia total. Desde luego, los intereses de los usuarios individuales son violados de alguna forma. Asimismo, en los sistemas operativos multitarea es imposible predecir el tiempo de ejecución de las aplicaciones, ya que ésta depende del número de las demás aplicaciones con las que el procesador debe compartir esta aplicación.

Para terminar esta sección, consulte la tabla 3.1 donde se resumen las propiedades de ambos tipos de red. Con base en esta información, se puede tomar una decisión bien fundamentada respecto a cuándo es más eficaz utilizar las redes de conmutación de circuitos y cuándo las de conmutación de paquetes.

TABLA 3.1 Propiedades de las redes de conmutación de circuitos y de paquetes

Conmutación de circuitos	Conmutación de paquetes
Antes de comenzar la transmisión de datos, es necesario establecer una conexión.	La necesidad de establecer una conexión no es obligatoria (método de datagramas).
La dirección se utiliza cuando se establece la conexión (establecimiento de la conexión).	La dirección junto con otra información de relleno se transmite en cada paquete.
La red puede rechazar la petición del usuario para establecer conexión.	La red siempre está lista para recibir datos del usuario.
El ancho de banda está garantizado para los usuarios que interactúan.	La velocidad de información no la conoce el usuario individual. Los retardos en la transmisión son aleatorios.
El tráfico en tiempo real es transmitido sin retardos.	Los recursos de la red se emplean eficazmente cuando se transmite tráfico en ráfagas.
Alta confiabilidad en la transmisión.	Existe pérdida de paquetes debido a la saturación de la memoria.
El uso ineficaz del ancho de banda reduce la eficacia total de la red.	Es posible la redistribución dinámica automática del ancho de banda de los enlaces físicos entre todos los usuarios de acuerdo con los requerimientos de su tráfico.

3.4 CONMUTACIÓN DE PAQUETES EN LAS REDES DE MEDIO COMPARTIDO

PALABRAS CLAVE: medio compartido, método de acceso aleatorio, PNA local, Ethernet, FDDI, *Token Ring*, adaptadores de red, tarjetas de interfase de red, monopolización, método de acceso determinístico, estafeta de acceso, marcador, repetidor de colisiones, hub, concentrador, puente, switch, estructura física de la red, enlaces lógicos de la red, estructura lógica de la red, cuello de botella y segmento lógico.

Anteriormente en este capítulo mencionamos los principios de compartir un enlace entre varias interfases o, en otras palabras, los principios para compartir un medio de transmisión. Ahora, permítanos explicar cómo trabajan estos principios en las LAN de conmutación de paquetes.

La compartición del medio de transmisión ha sido el concepto de LAN más popular por largo tiempo: este principio es la base de tecnologías modernas como Ethernet, FDDI y *Token Ring*; sin embargo, se puede llegar a la conclusión de que las redes basadas en medios de transmisión compartidos han rebasado el pico de su popularidad. Actualmente, Ethernet conmutado es la tecnología prevaleciente en el campo de las LAN. Por otro lado, el mundo de la conectividad de redes cambia tan rápido que la evidencia de revivir el interés en las tecnologías de medios compartidos cada vez es más notoria.

Ejemplos de nuevas áreas de aplicación de medios compartidos son las redes caseras cableadas, así como las redes inalámbricas personales y locales. La tecnología Home PNA ha surgido y está diseñada especialmente para usuarios domésticos. Dicha tecnología representa una modificación de la tecnología Ethernet estándar, en la cual se utiliza el cableado telefónico o eléctrico como medio compartido. Las redes personales de radio basadas en la tecnología Bluetooth, diseñadas para interconectar todos los dispositivos personales de alta tecnología (además de las computadoras de escritorio, esta lista incluye las PDA, los teléfonos móviles, las televisiones de alta tecnología y aun refrigeradores), también aplican el principio de medio de transmisión compartido.

Asimismo, las LAN Radio-Ethernet han surgido y están ganando popularidad rápidamente. Estas redes se emplean para conectar usuarios a Internet en aeropuertos, estaciones de ferrocarril y otros lugares donde se congregan usuarios móviles en grandes cantidades. Sin embargo, como nada es en realidad novedoso, recuerde que el Ethernet convencional se originó a partir de la red de radio ALOHA diseñada en la Universidad de Hawai, en la que un medio de transmisión compartido fue probado por primera vez. Simplemente, se vio que el aire no iba a ser un medio apropiado en los estándares de Ethernet por un largo tiempo, aunque siempre hubo algunos productos exóticos de determinadas compañías disponibles en el mercado. Con la llegada de Radio-Ethernet a finales de la década de 1990 se recuperó la justicia histórica.

3.4.1 Fundamentos de la compartición del medio de transmisión

Un **medio de transmisión compartido** es un medio físico que se utiliza en la transmisión de datos, al cual están conectados directamente muchos nodos terminales de la red y en el que solamente éstos pueden utilizarlo por turnos. Esto significa que en un momento dado, sólo uno de los nodos terminales puede tener acceso al medio compartido y lo utiliza para transmitir paquetes a otro nodo conectado al mismo medio de transmisión.

En la lista de posibles tipos de medio de transmisión compartido se incluyen el cable coaxial, el par trenzado, la fibra óptica y las ondas de radio.

Uno de los posibles métodos para compartir el medio de transmisión es el principio que sirve como base de la tecnología Ethernet: el **método de acceso aleatorio**. En este caso, el control de acceso al canal de comunicaciones es descentralizado; todas las interfases de red participan en este proceso. En particular, en las computadoras, el acceso a un medio compartido lo proporcionan controladores especiales llamados **adaptadores de red** o **tarjetas de interfase de red**.

A continuación se presenta la idea del método de acceso aleatorio:

- Las computadoras en dicha red pueden transmitir datos a través de la red solamente si está disponible el medio de transmisión; es decir, si no se llevan a cabo operaciones de

intercambio de datos entre computadoras y no existen señales eléctricas (ópticas) que viajen a través del medio.

- Después de asegurarnos de que el medio de transmisión está disponible, la computadora comienza la transmisión de datos, **monopolizando** de esta forma el medio de transmisión. El tiempo de acceso exclusivo al medio compartido proporcionado a un solo nodo está limitado por el tiempo necesario para transmitir una sola trama.
- Cuando se proporciona la trama al medio de transmisión, todos los adaptadores de red comienzan a recibir de manera simultánea esta trama. Cada adaptadora inspecciona la dirección de destino que se encuentra en uno de los campos iniciales de la trama.
- Si la dirección coincide con la de determinado adaptador, la trama se colocará en la memoria interna del adaptador de red. Por tanto, la computadora de destino recibe los datos que le fueron enviados.

Cuando se utiliza el método de acceso aleatorio, es posible que se presenten situaciones en las que dos o más computadoras decidan simultáneamente que la red está libre y comiencen a enviar información. Esta situación, conocida como **colisión**, representa un obstáculo para la transmisión de datos correcta a través de la red. Las señales provenientes de varios transmisores se sobreponen y distorsionan la señal resultante. Todas las tecnologías de red basadas en un medio compartido proporcionan un algoritmo para la detección y manejo adecuado de las colisiones. La probabilidad de que se presenten colisiones depende de la intensidad del tráfico.

Después de detectar una colisión, los adaptadores de red que intentaron enviar sus tramas detienen su transmisión, esperan un tiempo aleatorio y después, una vez más, tratan de acceder al medio y retransmitir la trama que provocó la colisión.

El **método de acceso determinístico** representa otra forma de acceder al medio de transmisión compartido. Este método se basa en el uso de una trama especial, generalmente conocida como **marcador** o **estafeta de acceso**. La computadora tiene el derecho a acceder al medio de transmisión solamente cuando posee la estafeta. El tiempo durante el cual la computadora puede tener a su disposición la estafeta es limitado; por tanto, después de que se vence este tiempo, la computadora está obligada a enviar la estafeta a otra computadora.

La regla que define el orden de la circulación de la estafeta debe garantizar el acceso de cada computadora al medio compartido durante un espacio constante de tiempo.

El método de acceso determinístico podrá implantarse si se utiliza un esquema centralizado o descentralizado. En el primer caso, la red no cuenta con un nodo en especial que defina la cola para acceder al medio compartido; en el segundo caso, existe dicho nodo y se conoce como el árbitro de acceso.

3.4.2 Razones de la estructuración de las LAN

Las primeras LAN estaban constituidas por un pequeño número de computadoras (generalmente de 10 a 30) y utilizaban un solo medio de transmisión compartido entre todos los dispositivos que formaban parte de la red. Al mismo tiempo, debido a limitaciones tecnológicas, las redes tenían topologías típicas: bus común (estrella) para Ethernet o anillo para FDDI y *Token Ring*. Estas topologías se caracterizan por la propiedad de homogeneidad (es decir, las computadoras de dichas redes son iguales al nivel de enlaces físicos). Dicha homogeneidad en cuanto a estructura simplifica el procedimiento de aumentar el número de computadoras, a la vez que simplifica la operación y el mantenimiento de la red.

Sin embargo, cuando se instalan redes de gran tamaño, tener una estructura homogénea de enlaces representa una desventaja. En dichas redes, el uso de estructuras típicas se convierte en una fuente de limitaciones, entre las cuales las más importantes son las siguientes:

- Limitaciones en cuanto a la longitud del enlace entre los nodos de la red
- Limitaciones en el número de nodos de la red
- Limitaciones en la intensidad de tráfico generado por los nodos de la red

Por ejemplo, la tecnología Ethernet basada en el uso de cable coaxial delgado permitía emplear tramos de cable no mayores que 185 metros a los cuales es posible conectar no más de 30 computadoras. Sin embargo, cuando las computadoras comenzaron a intercambiar información de una manera intensa, su número tuvo que reducirse a 20 o aun a 10. Esto fue necesario para garantizar que cada computadora recibiera una porción aceptable de ancho de banda total disponible en la red.

Con el fin de eliminar estas limitaciones, las redes se estructuraron con base en equipo de comunicaciones que contara con una estructura especializada:

- Repetidores
- Concentradores
- Puentes
- Switches

3.4.3 Estructura física de las LAN

Es necesario distinguir entre la topología de los enlaces físicos de la red (**estructura de la red física**) y la topología de los enlaces lógicos de la red (**estructura lógica de la red**).

La configuración de los enlaces físicos se define mediante las conexiones eléctricas (u ópticas) entre las computadoras, y puede representarse en la forma de una gráfica cuyos nodos son computadoras y equipos de comunicaciones y cuyas costillas corresponden a secciones de cable que conectan pares de nodos. Los enlaces lógicos corresponden a las rutas a lo largo de las cuales viajan los flujos de información a través de la red. Dichos enlaces lógicos generan la configuración adecuada del equipo de comunicaciones.

En algunos casos, las topologías física y lógica coinciden. Por ejemplo, la red que se muestra en la figura 3.15*a* tiene una topología física en anillo. Suponga que las computadoras que participan en esta red utilizan un método de acceso de estafeta circulante. La estafeta siempre se pasa secuencialmente de una computadora a otra en el orden correspondiente al que las computadoras usan para formar un anillo físico. Esto significa que la computadora A pasa la estafeta a la computadora B, esta última la pasa a la computadora C, y así sucesivamente. En este caso, la topología lógica de la red representa una topología en anillo.

La red que se muestra en la figura 3.15*b* ilustra el caso en el que las topologías física y lógica de la red no coinciden. Físicamente, las computadoras están conectadas de acuerdo con la topología en bus (estrella) común; sin embargo, el acceso al bus no cumple con el algoritmo de acceso aleatorio utilizado en la topología Ethernet. Por el contrario, se lleva a cabo pasando la estafeta en un orden tal que forma un anillo; de la computadora A a la B, de la B a la C, etc. Aquí, el orden en que se circula la estafeta no refleja el orden de los enlaces físicos; en lugar de eso, está determinado por la configuración lógica de los controladores de los adaptadores de red. Nada nos prohíbe configurar los adaptadores de red y sus controladores de manera tal que las computadoras formen un anillo con otro orden, por ejemplo: B, A y C; sin embargo, en todos estos casos, la estructura física de la red no cambia.

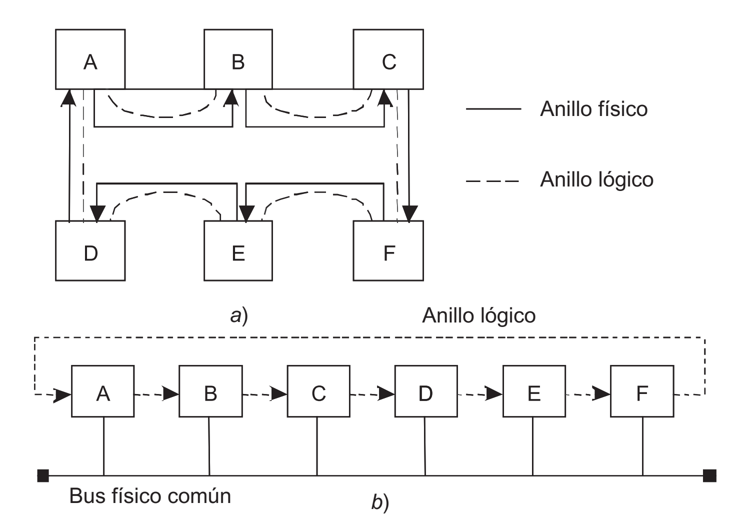


FIGURA 3.15 Topologías lógica y física de la red.

La estructuración física del medio de transmisión compartido representa el primer paso para construir LAN de alta calidad. El objetivo de la estructuración física es garantizar la posibilidad de construir la red a partir de secciones físicas de cable, en lugar de hacerlo con base en una sola sección de cable. Teniendo en cuenta todo lo anterior, estas secciones físicamente distintas tenían que continuar trabajando como un medio común compartido de transmisión (es decir, desde el punto de vista lógico, tenían que conservarse idénticas).

Las formas principales de estructurar físicamente las LAN son los repetidores y concentradores o hubs.

Un **repetidor** es el dispositivo de comunicaciones más simple utilizado para conectar físicamente diversos segmentos del cable LAN con el fin de incrementar la longitud total de la red. Los repetidores retransmiten las señales provenientes de un segmento de red a otros segmentos (figura 3.16), mejorando de manera simultánea sus características físicas. Por ejemplo, un repetidor amplifica la señal y mejora su forma y sincronía. Para realizar esto último se corrige la falta de uniformidad de los intervalos entre pulsos. De esta forma, el repetidor supera las limitaciones en cuanto a la longitud de los enlaces de comunicaciones. Como el flujo se las señales que son transmitidas por el nodo hacia la red se propagan a través de todos los segmentos de la red, dicha red conserva las propiedades de una red con medio de transmisión compartido.

Un repetidor que tenga varios puertos y conecta varios segmentos físicos suele llamarse **concentrador** o **hub**. Estos nombres dan a entender que todos los enlaces entre los segmentos de red están concentrados en este dispositivo.

IMPORTANTE *La adición de concentradores a la red siempre modifica la topología física, pero deja inalterada su topología lógica.*

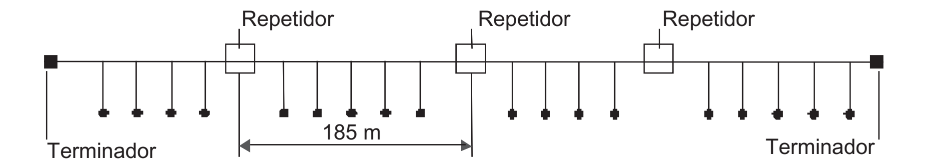


FIGURA 3.16 Los repetidores permiten un aumento en la longitud de la red Ethernet.

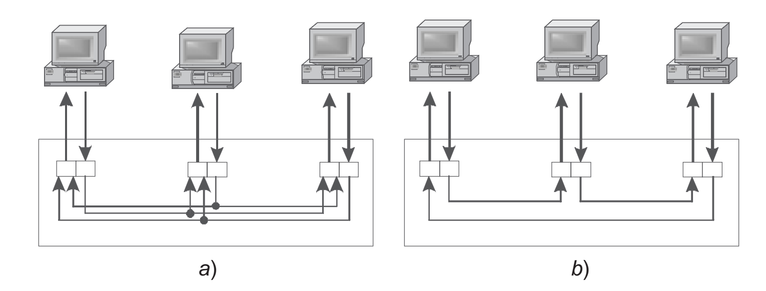


FIGURA 3.17 Concentradores de diferentes tecnologías.

Los concentradores son dispositivos obligados en prácticamente todas las tecnologías básicas de las LAN: Ethernet, Arcnet, *Token Ring*, FDDI, Fast Ethernet, Gigabit Ethernet y 100VG-AnyLAN.[3]

Es necesario hacer énfasis en que la operación de los concentradores en cualquier tecnología tiene mucho en común. Éstos repiten las señales provenientes de uno de sus puertos a los demás. De hecho, estos puertos repiten las señales entrantes que hacen la diferencia; por tanto, el concentrador de Ethernet repite las señales de entrada que llegan a todos sus puertos, excepto al puerto por el cual llegaron las señales (figura 3.17*a*). Por otro lado, el concentrador *Token Ring* (figura 3.17*b*) repite las señales de entrada que llegan a alguno de sus puertos hacia uno de sus puertos solamente; es decir, hacia el puerto al cual está conectada la siguiente computadora dentro del anillo.

3.4.4 Estructura lógica de una red de medio compartido

La estructuración física de una red no puede resolver problemas tan importantes como la escasez del ancho de banda y la imposibilidad de utilizar enlaces de comunicaciones con múltiples anchos de banda en diferentes segmentos de la red. Para este caso, podría ser de ayuda una estructuración lógica de la red.

Una típica topología de red física (bus, anillo o estrella), la cual limite todos los dispositivos de la red proporcionándoles un medio de transmisión compartido para el intercambio de datos, no es adecuada para estructurar los flujos de información en una red de gran tamaño. Por ejemplo, en la red de bus común, cualquier par de computadoras que interactúan monopoliza el canal de comunicaciones durante todo el tiempo del intercambio de datos. Por tanto, a medida que el número de computadoras de la red aumenta, el bus se convierte en un cuello de botella.

EJEMPLO *Suponga que una empresa tuvo una red Ethernet extremadamente simple, con sólo un segmento (figura 3.18). Todas las computadoras de la empresa estaban conectadas a un cable coaxial. Con el tiempo, el número de usuarios aumentó y la red se saturaba con mucha frecuencia. En consecuencia, los usuarios tenían que esperar más tiempo para que respondieran las aplicaciones de red; además, las limitaciones en cuanto a la longitud de los enlaces de conexión entre computadoras se hicieron muy notorias, pues se vio que era imposible colocar todas las computadoras dentro de las instalaciones asignadas a un nuevo grupo de trabajo. Se tomó una decisión*

---

[3] No todas las tecnologías listadas han conservado su importancia. Por ejemplo, Arcnet y 100VG-anyLAN pueden considerarse solamente ejemplos de las soluciones técnicas originales.

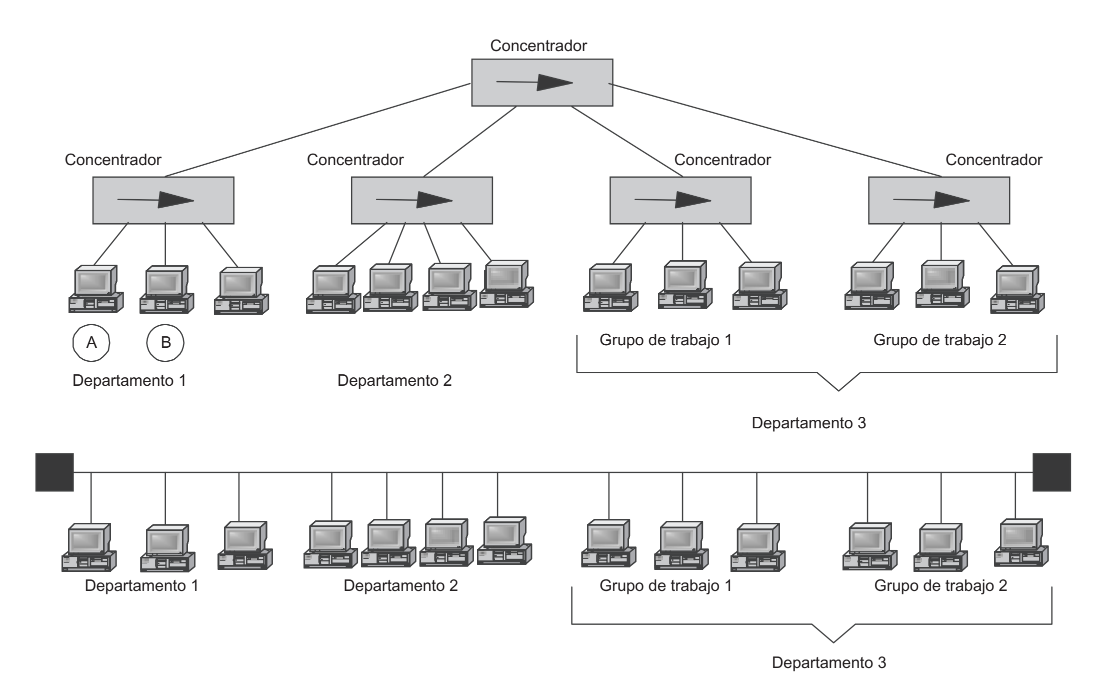


FIGURA 3.18 La reestructuración física de la red no mejora su desempeño.

en cuanto al uso de concentradores. La red reconstruida que se obtuvo como resultado de esta restructuración física se muestra en la parte superior de la figura 3.18. Ahora fue factible colocar las computadoras a una distancia mayor y la estructura física de la red estaba de acuerdo con la estructura administrativa de la empresa; sin embargo, los problemas relacionados con el desempeño quedaron sin resolver. Por ejemplo, en cualquier momento que el usuario de la computadora A enviaba datos a su usuario vecino B, se saturaba toda la red. Esto no es una sorpresa pues, de acuerdo con la lógica de la operación del concentrador, la trama enviada por la computadora A hacia la B se repetía en todas las interfases de todos los nodos de la red. Esto significa que hasta que la computadora B recibía la trama dirigida a ella, ninguna otra computadora de esta red podía acceder al medio de comunicaciones compartido. Tal situación surgió debido a que el uso de concentradores modificó solamente la estructura física de la red, sin cambiar su estructura lógica (parte inferior de la figura 3.18), de acuerdo con la cual la información continuaba propagándose hacia toda la red, donde todas las computadoras tenían el mismo derecho a acceder al medio de comunicaciones, independientemente de su ubicación.

La solución a este problema consiste en olvidar la idea de usar el medio de transmisión compartido para todos los nodos. Por tanto, en el ejemplo que se estudió en la figura 3.18, hubiera sido conveniente asegurar que las tramas transmitidas por las computadoras pertenecientes al departamento 1 nunca se salen de los límites de esta parte de la red, excepto cuando éstas estuvieran dirigidas a cualquier computadora que perteneciera a otro departamento. Por otro lado, sólo aquellas tramas dirigidas a los nodos del departamento en particular deben transferirse a su red. Así, dentro de los límites de cada departamento, se utiliza un medio de transmisión compartido independiente, el cual es "propiedad" de ese departamento.

IMPORTANTE *La propagación del tráfico dirigido a un segmento específico de la red que esté solamente dentro de los límites de dicho segmento se conoce como localización del*

tráfico. La estructuración lógica de la red es el proceso que consiste en dividir la red en segmentos con tráfico localizado.

Dicha forma de organizar la red mejorará de manera significativa el desempeño de ésta, pues las computadoras de un departamento no tendrán que esperar mientras que las computadoras de otros departamentos intercambian datos. Además, la estructuración lógica permite que el ancho de banda disponible sea diferenciado en varias partes de la red.

La **estructuración lógica** de la red se logra mediante el uso de puentes, switches, ruteadores y puertas de acceso.

Un **puente** divide el medio de transmisión compartido en partes (a menudo llamadas **segmentos lógicos**) y transmite información de segmento a segmento sólo cuando es necesaria dicha transmisión; es decir, cuando la dirección de la computadora de destino pertenece a otro segmento (figura 3.19). Haciendo lo anterior, el puente aísla el tráfico de un segmento del tráfico de otro segmento y de esta forma mejora el desempeño total de la red. La localización de tráfico no solamente utiliza el ancho de banda de manera más moderada, sino también reduce la posibilidad de acceso no autorizados a los datos. Como las tramas no se salen de los límites de su segmento es más difícil que los intrusos las intercepten.

La figura 3.20 muestra la red que se obtiene a partir de una red con un concentrador central (consulte la figura 3.19) y reemplaza el concentrador central con un puente. Cada red de los departamentos 1 y 2 forma un segmento lógico, mientras que la red del departamento

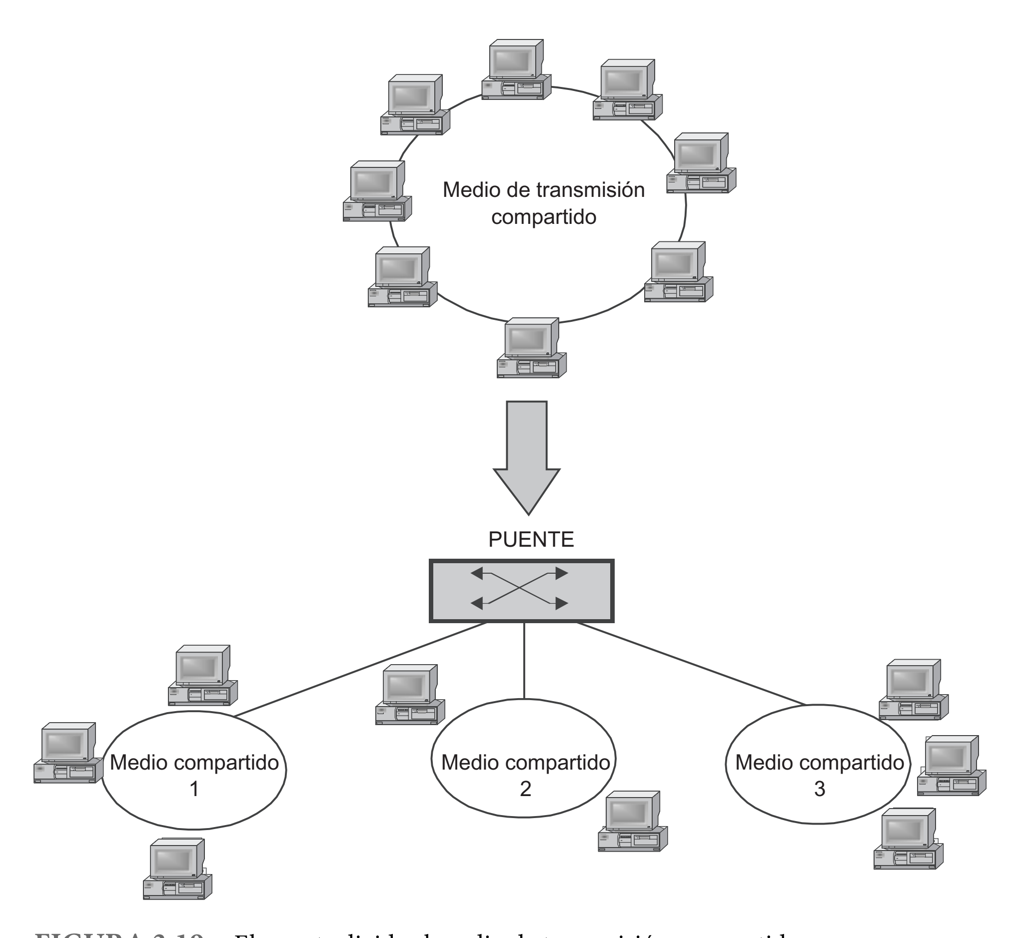


FIGURA 3.19 El puente divide el medio de transmisión compartido.

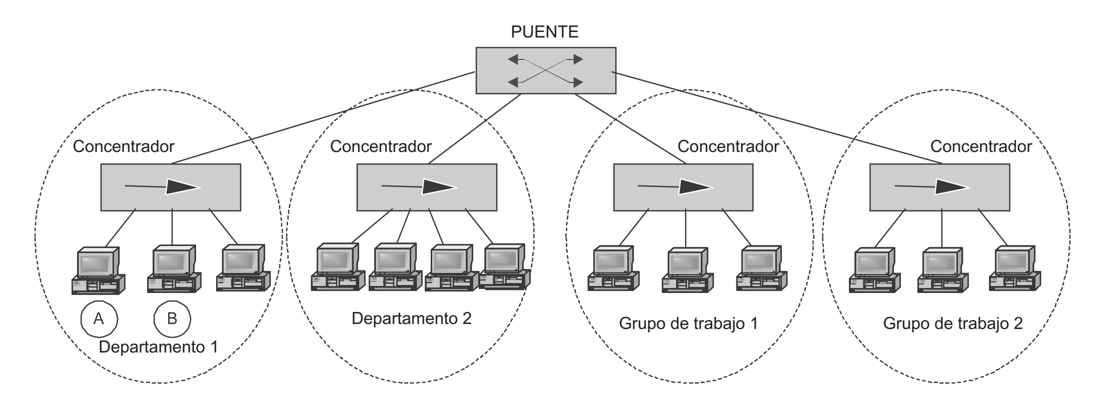


FIGURA 3.20 Estructuración lógica de la red: utilizando un puente, un medio compartido se divide en cuatro medios compartidos independientes.

3 tiene dos segmentos lógicos. Cada segmento lógico se basa en el concentrador y tiene la estructura física más simple formada por las secciones de cable que conectan las computadoras a los puertos del concentrador. Si el usuario que trabaja en la computadora A envía datos al usuario de la computadora B localizada dentro del mismo segmento, estos datos serán repetidos solamente en las interfases de red marcadas con círculos.

Para la localización de tráfico, los puentes utilizan las direcciones de hardware de las computadoras. Uno se puede hacer la pregunta: ¿cómo sabe el puente a qué interfase debe enviar la trama? Después de todo, las direcciones de hardware no contienen información alguna acerca del segmento al cual pertenece la computadora con la dirección específica. Ciertamente, el administrador de la red puede especificar esta información al puente mediante su configuración en forma manual; sin embargo, este método no es conveniente en el caso de redes de gran tamaño. El puente resuelve este problema de modo automático por medio de la implantación de un simple algoritmo de aprendizaje.

Todas las tramas que se dirijan hacia una interfase específica son generadas por las computadoras que pertenecen al segmento conectado a dicha interfase. El puente recupera las direcciones del emisor a partir de las tramas entrantes y las coloca en una tabla especial, en la que se determina también la interfase por la cual la trama específica llegó; por tanto, el puente determina qué computadoras están conectadas a cada interfase. Después, el puente utiliza esta información para enviar la trama exactamente hacia esa interfase, a través de la cual pasa la ruta hacia la computadora de destino. Como el puente no conoce la topología exacta que forman los enlaces entre los segmentos lógicos de la red, éste puede operar de manera correcta solamente en aquellas redes donde los enlaces entre segmentos no formen loops.

El *switch LAN* es funcionalmente similar al puente. (En este contexto, el término *switch* se utiliza en un sentido restringido, para expresar un switch LAN.) Su diferencia principal respecto al puente estriba en su mejor desempeño. Cada interfase del switch cuenta con un procesador especializado que procesa las tramas utilizando el mismo algoritmo que se empleó en el puente, independientemente de los procesadores de los demás puertos. Debido a esta característica, el desempeño total del switch es, en general, significativamente más alto que el del puente convencional, el cual cuenta sólo con una unidad de procesamiento. Se puede decir que los switches son puentes avanzados que procesan las tramas de modo paralelo. Cuando el uso de procesadores especializados en cada puerto, de un dispositivo de comunicaciones, se justifica desde el punto de vista económico, los switches reemplazan a los puentes.

3.4.5 Ethernet como ejemplo de una tecnología estándar

Considere cómo los métodos generales para resolver los problemas más importantes que se pueden encontrar en la construcción de redes están implementados en una de las primeras tecnologías estándares de red: Ethernet basada en un medio de transmisión compartido. En esta sección se estudiarán solamente los principios generales, los cuales forman las bases de una de las variantes de Ethernet. En la parte III de este libro se hacen descripciones detalladas de todos los tipos de Ethernet, incluido Ethernet conmutado.

Topología. El estándar Ethernet define estrictamente la topología de los enlaces físicos: el *bus común* (figura 3.21). Dicha figura muestra la implementación más simple de esta topología, la cual comprende un solo segmento al que se conectan todas las computadoras hacia el medio de transmisión compartido.

Método de conmutación. La red Ethernet utiliza conmutación de paquetes de datagrama. En Ethernet, la unidad de datos empleada para el intercambio de datos se expresa como trama. Desde el punto de vista funcional, una trama es idéntica a un paquete, tiene un formato fijo y, además del campo de datos, contiene información extra.

¿Y dónde está la red de conmutación en la red Ethernet de un solo segmento?, ¿existe al menos un switch que, como ya se mencionó, represente el elemento principal de cualquier red de conmutación de paquetes?, ¿es probable que Ethernet represente un tipo especial de conmutación?

En realidad, hay un switch en una red Ethernet de un solo segmento, aunque sea muy difícil detectarlo debido a que sus funciones se encuentran distribuidas a lo largo de toda la red. Este "switch" Ethernet incluye adaptadores de red y un medio de transmisión compartido. Los adaptadores de red son las interfases de dicho switch virtual; el medio de transmisión compartido desempeña el papel de la unidad de conmutación que transmite las tramas entre las interfases. Los adaptadores también llevan a cabo las funciones de la unidad de conmutación, ya que éstos deciden cuál trama está dirigida a la computadora local y cuál no lo está.

Direccionamiento. Cada computadora —o, para ser más precisos, cada adaptador de red— tiene una dirección única en su hardware. Dicha dirección se conoce como *dirección MAC*, la cual se mencionó anteriormente. Una dirección Ethernet es una dirección numérica plana puesto que no se utiliza una jerarquía en este caso. Los siguientes tipos de direcciones son soportados: unidirigida, difundida ampliamente y multidirigida.

Compartición y multiplexaje del medio de transmisión. Los nodos terminales utilizan un solo medio de transmisión compartido para el intercambio de datos, mediante el uso de un método de acceso aleatorio.

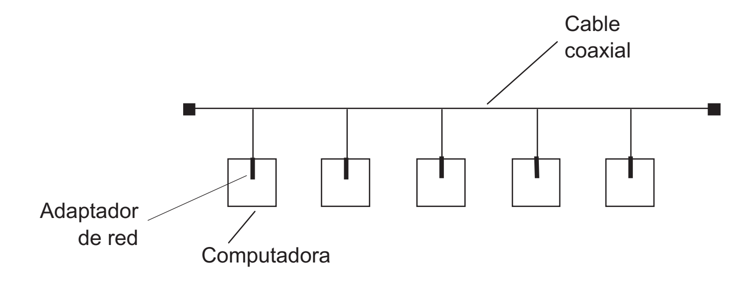


FIGURA 3.21 Red Ethernet.

Los flujos de información provenientes de los nodos terminales de Ethernet son multiplexados para formar un único enlace de transmisión con base en tiempo compartido. Esto significa que las tramas que pertenecen a los diferentes flujos obtienen el acceso al enlace tomando turnos. Para destacar la diferencia entre los conceptos de multiplexaje y compartición del medio de transmisión, la cual no siempre es obvia, considere la situación en la que sólo una de las computadoras conectadas a Ethernet necesite transmitir datos, los cuales normalmente son generados por varias aplicaciones. En este caso, no se presenta el problema de la compartición del medio de transmisión entre las interfases de red; el problema que representa la transmisión de varios flujos de información a través de un enlace común (es decir, el problema del multiplexaje) aún está sin resolver.

Codificación. Los adaptadores de Ethernet trabajan a una frecuencia de reloj de 20 MHz transmitiendo a través del medio de transmisión pulsos rectangulares correspondientes a unos y ceros binarios. Cuando comienza la transmisión de las tramas, todos sus bits se envían hacia la red a una velocidad constante igual a 10 Mbps. La transmisión de cada bit implica usar dos relojes. Esta velocidad es el ancho de banda del enlace en Ethernet.

Confiabilidad. Para mejorar la confiabilidad de la transmisión de datos, Ethernet utiliza técnicas estándar, las cuales incluyen el cálculo de la suma verificadora y su transmisión en el remolque (trailer) de la trama. Si el adaptador del receptor detecta un error en los datos de la trama al recalcular la suma verificadora, eliminará dicha trama. El protocolo Ethernet no retransmite la trama; esta tarea se delega a otras tecnologías (por ejemplo, al protocolo TCP en las redes TCP/IP).

El método de transmisión half-dúplex. El medio de transmisión compartido de Ethernet representa un canal de comunicaciones half-dúplex. En realidad, el adaptador de red no puede utilizar este canal de manera simultánea para transmitir y recibir datos. Dichas tareas deben llevarse a cabo una a la vez.

Colas. Al principio, podría parecer que en la red Ethernet basada en un medio compartido no hubiera las colas que caracterizan a las redes de conmutación de paquetes; sin embargo, la falta de un switch con memoria de almacenamiento en dichas redes no significa que no haya colas. Simplemente, en este caso, las colas han sido enviadas a la memoria de almacenamiento de los adaptadores de red. Cuando el medio de transmisión se encuentra ocupado transmitiendo tramas a otros adaptadores de red, los datos (la carga ofrecida) continúan llegando al adaptador de red. Como en ese momento los datos no pueden transmitirse a la red, éstos comienzan a acumularse en la memoria interna del adaptador de Ethernet y forman de esta manera una cola. Por tanto, de manera similar a las demás redes de conmutación de paquetes, en la red Ethernet se presentan retardos variables en la entrega de tramas.

Sin embargo, Ethernet también tiene una característica específica. El medio de transmisión compartido es un tipo de regulador de la velocidad de transmisión de tramas y cuando está ocupado no recibe más tramas. Por ende, la red ejerce presión hacia atrás cuando está muy saturada y de esta forma fuerza a los nodos terminales a reducir su velocidad de transmisión de datos hacia la red.

RESUMEN

- En las redes de conmutación de circuitos se crean canales de información continuos, conocidos como *circuitos a solicitud de los usuarios*. El circuito se forma reservando una cadena de enlaces de comunicaciones que conectan a los usuarios por el tiempo en que se lleva a cabo la transmisión de datos. A lo largo de toda su longitud, el circuito transmite datos a una velocidad constante. Esto significa que la red de conmutación de

circuitos puede garantizar la transmisión con alta calidad de datos sensibles al retardo (voz y video) también conocido como tráfico en tiempo real; sin embargo, la imposibilidad de redistribuir dinámicamente el ancho de banda del enlace físico representa una limitante en las redes de conmutación de circuitos. Dicha limitante hace que este tipo de redes sea ineficaz en la transmisión de tráfico en ráfagas, el cual es típico en las redes de computadoras.

- Cuando se usa la conmutación de paquetes, el nodo de origen divide los datos que se van a transmitir en pequeños fragmentos, conocidos como *paquetes*. El paquete se genera con un encabezado que especifica la dirección de destino. Por tanto, éste puede ser procesado por el switch independientemente de los demás datos. El método de la conmutación de paquetes mejora el desempeño de la red cuando se transmite tráfico en ráfagas, debido a que cuando atiende a una gran cantidad de flujos independientes, sus periodos de actividad no siempre coinciden. Los paquetes son transmitidos hacia la red sin que ésta haya tenido que reservar previamente recursos, a la velocidad a la que los paquetes son generados por la fuente; sin embargo, este método de conmutación tiene su lado oscuro: los retardos en la transmisión son de naturaleza aleatoria; por tanto, se presentan problemas en el curso de la transmisión de tráfico en tiempo real.
- Las redes de conmutación de paquetes pueden utilizar uno de los tres algoritmos de direccionamiento: sin el establecimiento de una conexión (no orientado a la conexión), también conocido como *transmisión de datagramas*; orientado a la conexión, y circuito virtual.
- Un medio de transmisión compartido es un medio físico para la transmisión de datos (cable coaxial, par trenzado, fibra óptica u ondas de radio) al que un número específico de nodos terminales de la red están conectados directamente, el cual sólo puede utilizar tomando turnos. El principio de compartición del medio de transmisión constituye la base de tecnologías muy conocidas, como Ethernet, FDDI y *Token Ring*. Aunque aparentemente las redes basadas en un medio de transmisión compartido hayan sobrevivido su pico de popularidad, algunas señales indican que existe interés por revivir dicha tecnología. Por ejemplo, nuevas tecnologías como las redes caseras y las redes inalámbricas personales y locales aplican el principio del medio de transmisión compartido.

PREGUNTAS DE REPASO

1. ¿Qué tipos de multiplexado y conmutación son utilizados en las redes telefónicas?
2. ¿Qué propiedades de las redes de conmutación de circuitos pueden considerarse desventajas?
3. ¿Qué propiedades de las redes de conmutación de paquetes afectan de forma adversa la transmisión de información multimedia?
4. ¿Se utiliza el almacenamiento en memoria en las redes de conmutación de circuitos?
5. ¿Qué elemento de la red de conmutación de circuitos puede negar la solicitud de un nodo para establecer un circuito?
   a) Ninguno, la red está lista siempre para recibir datos provenientes de un usuario.
   b) Cualquier nodo transmisor.
   c) El nodo de destino.
6. ¿Qué conceptos son característicos de la tecnología Ethernet?
7. ¿Tienen en cuenta las redes de datagramas los flujos existentes?
8. Dé la definición de una conexión lógica.

9. ¿Es posible proporcionar una transferencia de datos confiable sin una conexión lógica entre nodos terminales?

10. ¿Qué conexiones lógicas podrían llamarse *circuito virtual*?

11. ¿Cuáles redes usan la teconología del circuito virtual?

12. Especifique cuáles de los dispositivos listados a continuación son funcionalmente similares:

a) Hub
b) Switch
c) Concentrador
d) Repetidor
e) Ruteador
f) Puente

13. Liste las diferencias que existen entre un puente y un switch.

14. ¿Es verdadero el enunciado siguiente? La red Ethernet construida formando una topología estrella con el concentrador en el centro es más confiable que la misma red construida con cable coaxial y una topología de bus común.

15. ¿Cómo podría usted incrementar el ancho de banda disponible en la computadora de cada usuario en una red construida con base en concentradores?

PROBLEMAS

1. Determine cómo aumentará el tiempo de transmisión de datos en la red de conmutación de paquetes comparada con la red de conmutación de circuitos dadas por los datos siguientes:

- Cantidad total de los datos trasmitidos: 200 KB
- Longitud total del enlace de conexión: 5 000 km
- Velocidad asumida de propagación de la señal: 0.66 veces la velocidad de la luz.
- Ancho de banda del enlace: 2 Mbps
- Tamaño de paquetes (sin tener en cuenta el tamaño del encabezado): 4 KB
- Tamaño del encabezado: 40 bytes
- Intervalo entre paquetes: 1 mseg
- Número de switches de tránsito: 10
- Tiempo de conmutación de cada switch: 2 mseg

Suponga que la red trabaja en modo con baja carga. Por tanto, no se forman colas en los switches.

2. Si todos los dispositivos de comunicaciones en el fragmento de red que se muestra en la figura 3.22 son concentradores, ¿en qué puertos aparecerá una trama enviada de la computadora A a la B?

1. 5 y 6
2. 4, 5 y 6
3. 4, 5, 6 y 7
4. 4, 5, 6, 7 y 12
5. En todos los puertos

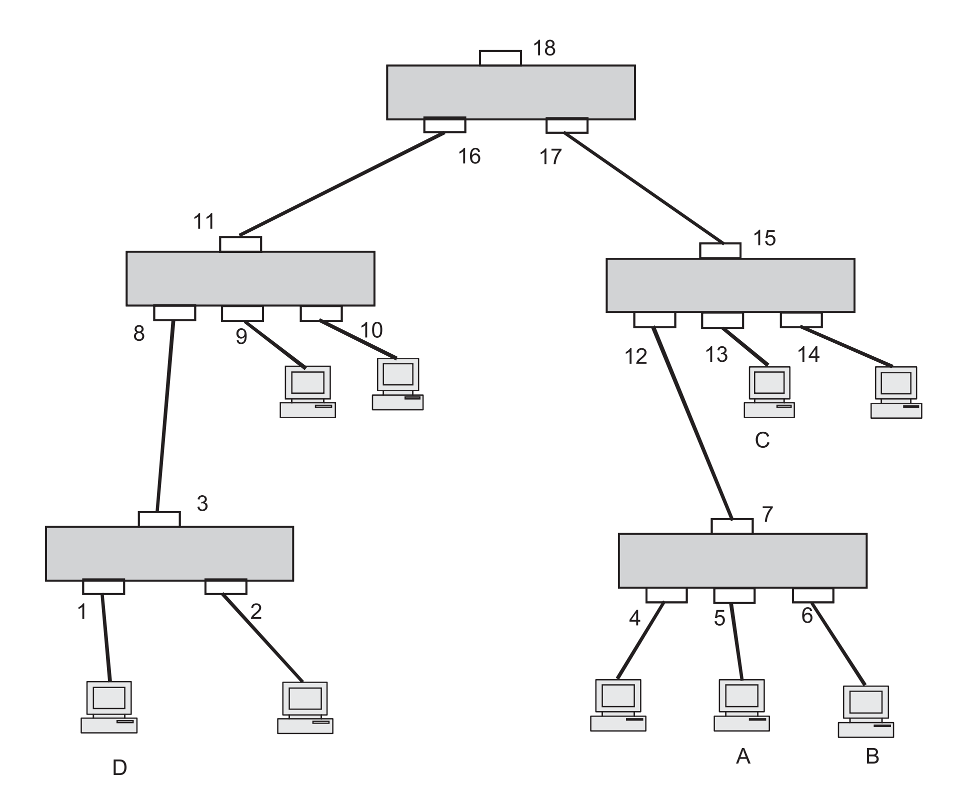


FIGURA 3.22 Fragmento de la red.

3. Siempre que todos los dispositivos de comunicaciones en el fragmento de red de la figura 3.22 representen switches, ¿en qué puerto aparecerá la trama enviada de la computadora A a la B?
4. Si todos los dispositivos de comunicaciones del fragmento de red de la figura 3.22 son switches, excepto un concentrador al que están conectados las computadoras A y B, ¿en qué puertos aparecerá una trama que se envía de la computadora A hacia la D?
5. En una red de datagramas, entre los nodos A y B existen tres flujos y tres rutas alternas. ¿Es posible enviar cada flujo a través de una ruta diferente?
6. En una red de circuitos virtuales, entre los nodos A y B existen tres flujos y tres rutas alternas. ¿Es posible enviar cada flujo a través de rutas diferentes?
7. Una red está basada en un medio de transmisión compartido con un ancho de banda de 10 Mbps y cuenta con 100 nodos. ¿Cuál será la velocidad máxima de transferencia de datos entre dos computadoras de dicha red?
8. Una red puede transmitir datos en dos modos: datagrama y circuito virtual. ¿Qué aspectos tendría usted en cuenta al seleccionar el modo específico de transmisión de datos si el criterio principal fuera la velocidad y la confiabilidad en la entrega de los datos?
9. ¿Considera usted que las redes de conmutación de circuitos serán reemplazadas en el corto plazo por las redes de conmutación de paquetes? O, por el contrario, ¿las redes de conmutación de paquetes serán reemplazadas por las de circuitos? O ¿ambas tecnologías pueden coexistir? Proporcione argumentos que fundamenten su opinión. Tenga en cuenta diferentes áreas de aplicación de estas tecnologías.

4

ARQUITECTURA Y ESTANDARIZACIÓN DE REDES

DESCRIPCIÓN DEL CAPÍTULO

4.1 INTRODUCCIÓN

La arquitectura de redes es una representación de la red como un sistema compuesto de varios elementos, cada uno de los cuales lleva a cabo una función específica. Todos los elementos de la red trabajan de manera coordinada con el fin de resolver la función común de interactuar entre las computadoras. En otras palabras, la arquitectura de red descompone un problema en una serie de subproblemas que los elementos individuales de la red deben resolver. Uno de los elementos más importantes de la arquitectura de red es el **protocolo de comunicaciones**, el cual puede definirse como el conjunto formal de reglas para la interacción entre los nodos de la red.

El desarrollo de la interconexión de sistemas abiertos (OSI, por sus siglas en inglés) fue un evento muy significativo en la estandarización de la arquitectura de las redes de computadoras. Dicho modelo, diseñado a principios de la década de 1980, resumió toda la experiencia acumulada de esa época. El modelo OSI representa un estándar internacional y define el método para descomponer *verticalmente* el problema de la interacción entre computadoras al delegar esta tarea a los protocolos de comunicaciones, los cuales se dividieron en siete capas. Las capas de los protocolos de comunicaciones forman una jerarquía conocida como **pilas de protocolos**, en la que cada capa utiliza la capa inferior como una herramienta apropiada para resolver sus tareas.

Las pilas de protocolos utilizadas en la actualidad (o las más populares hasta la fecha) reflejan en general la arquitectura del modelo OSI; sin embargo, cada pila de protocolos cuenta con características y diferencias específicas con respecto a la arquitectura del modelo OSI. De este modo, la pila TCP/IP más popular está formada por cuatro capas en lugar de siete.

La arquitectura estándar de las redes de computadoras también determina la distribución de protocolos entre los elementos de la red, tales como los nodos terminales (computadoras) y los nodos de paso (interruptores y ruteadores). Los nodos de paso solamente soportan un subconjunto limitado de las funciones de la pila de protocolos; éstos llevan a cabo funciones de transporte mediante la transmisión de tráfico de red entre los nodos terminales. Estos a su vez soportan toda la pila de protocolos, ya que deben proporcionar servicios de información, como el servicio web. Dicha distribución de funciones transfiere las funciones intelectuales de la red hacia la periferia de la misma.

4.2 DESCOMPOSICIÓN DE LA INTERACCIÓN DE LOS NODOS DE RED

PALABRAS CLAVE: descomposición, módulo, protocolo, método multicapas, interfase de servicio, interfase intercapas, interfase de igual a igual, pila de protocolos, conjunto de protocolos y suite de protocolos.

Organizar la interacción entre dispositivos de red es una tarea muy compleja. El método universal más conocido y común para resolver cualquier tipo de tareas complejas consiste en su **descomposición** (es decir, en la división de un problema complejo en varias tareas más sencillas o módulos). La descomposición implica definir de manera estricta las funciones de cada módulo, así como la forma como interactúan. Esto se conoce con el nombre de *interfase entre módulos*. Cuando se utiliza este método, cada módulo puede considerarse una *caja negra* al ser sustraída de sus mecanismos internos y al concentrar toda la atención en la forma como interactúan. Si se simplifica este problema de manera lógica, es factible

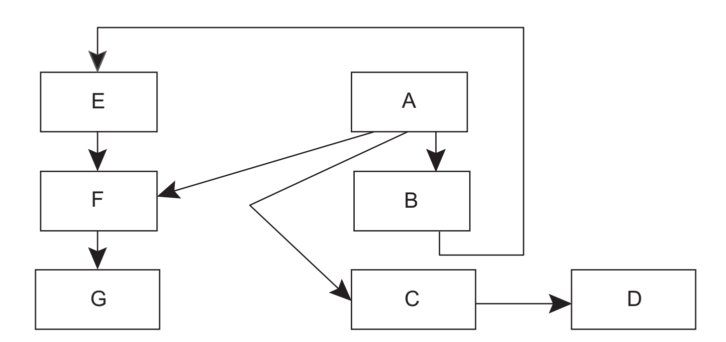


FIGURA 4.1 Ejemplo de un problema de descomposición.

desarrollar, modificar y probar cada módulo de manera independiente. Por lo tanto, cada módulo que se muestra en la figura 4.1 puede reescribirse sin necesidad de modificar los demás. Considere el módulo A. Siempre y cuando los desarrolladores hayan dejado las interfases entre módulos sin modificaciones (en tal caso, éstas serán las interfases A-B y A-C), no se requerirán cambios en los demás módulos.

4.2.1 Método multicapas

El **método multicapas** es un concepto aún más eficaz. Después de representar la tarea inicial como un conjunto de módulos, éstos se agrupan y ordenan por capas y forman una jerarquía. Cuando se utiliza el principio de la jerarquía para cada capa intermedia, es posible especificar directamente las capas contiguas arriba y debajo de ésta (figura 4.2).

Cuando lleva a cabo sus tareas, el grupo de módulos que forman cada capa debe requerir servicios solamente de los módulos de la capa inferior. Dichos módulos han de transferir los resultados de su operación sólo a los módulos que pertenezcan a la capa ubicada inmediatamente arriba de ellos. Esa descomposición jerárquica supone la definición clara de las funciones e interfases no sólo de los módulos específicos, sino también de cada capa.

La **interfase entre capas**, también conocida como **interfase de servicio**, define el conjunto de funciones que la capa inferior proporciona a la capa que se halla directamente arriba de ésta (figura 4.3).

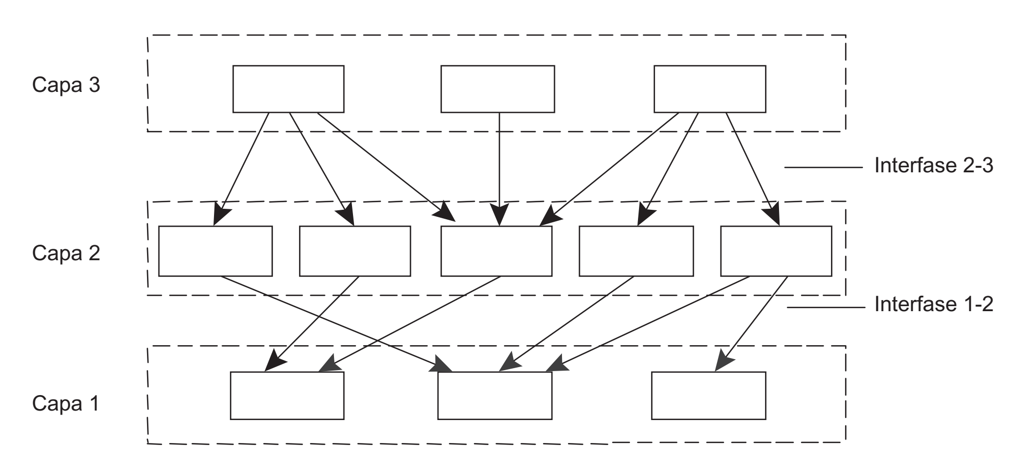


FIGURA 4.2 Método multicapa: creación de una jerarquía de tareas.

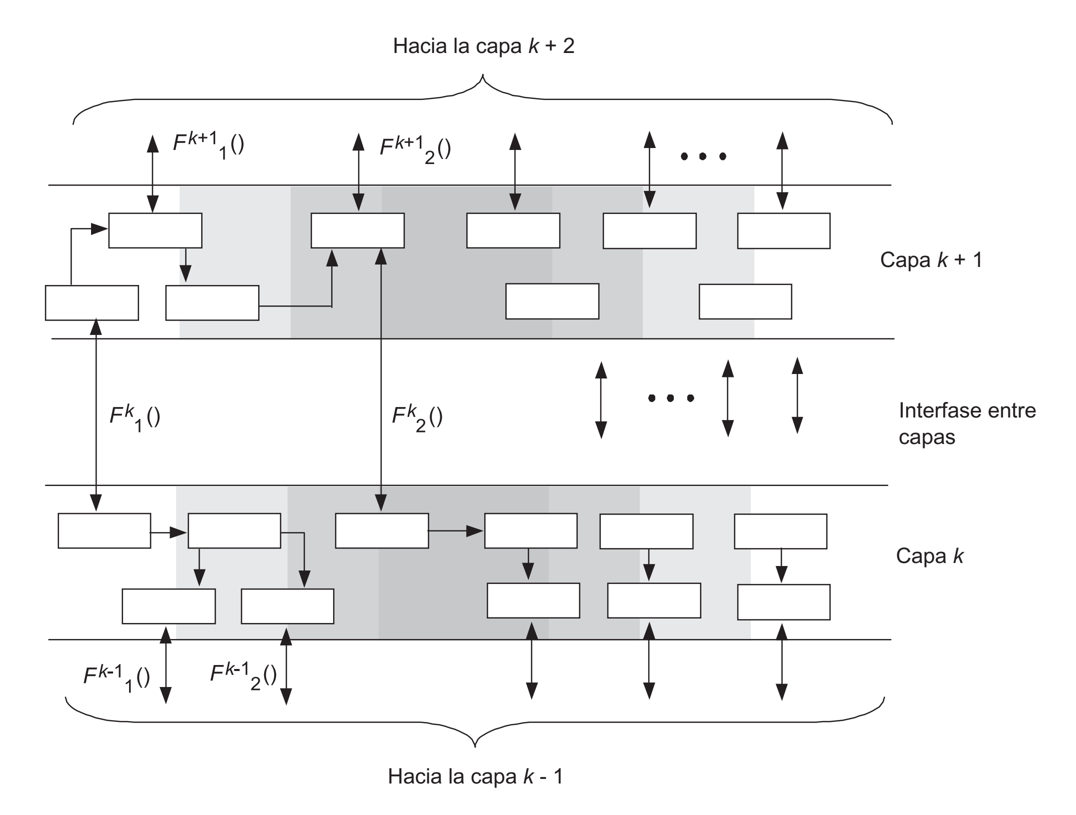


FIGURA 4.3 Concepto de la interacción entre multicapas.

Dicho método permite el desarrollo, prueba y modificación de capas específicas independientemente de las demás capas. Al moverse de las capas inferiores a las superiores, la descomposición jerárquica permite la creación de representaciones más abstractas de los problemas iniciales y, en consecuencia, más sencillas.

EJEMPLO *Considere la descripción simplificada de la tarea que consiste en la lectura de un registro lógico de un archivo almacenado en el disco duro. Esta tarea puede representarse como una jerarquía de las tareas específicas siguientes:*

1. *Mediante el uso de un nombre simbólico de archivo, busque las características del archivo que se requieren para acceder a los datos, tales como la ubicación física del archivo, su tamaño, etc. Como las funciones de esta capa están relacionadas solamente con la consulta del directorio, la representación de los sistemas de archivo en esta capa es muy abstracta. Un sistema de archivos se representa como un árbol cuyos nodos son directorios (carpetas) y cuyas hojas representan archivos. En esta capa no es de interés ningún otro detalle de la organización física o lógica de los datos en el disco duro.*
2. *En seguida es necesario determinar la parte específica del archivo que debe ser leída. Para llevar a cabo esta tarea, diríjase a la capa de abstracción más inferior del sistema de archivos. Las funciones de esta capa interpretan los archivos como conjuntos de bloques físicos del disco, relacionados entre sí de manera específica.*
3. *Por último, lea los datos del disco que se requieran. Después de determinar el número de bloque físico, el sistema de archivos solicita al sistema de entrada/salida*

que realice la operación de lectura. En este nivel, se debe lidiar con los detalles del sistema de archivos, tales como el número de cilindros, pistas y sectores.

Por ejemplo, entre las funciones que las aplicaciones deben llamar cuando solicitan a las capas superiores del sistema de archivos, es probable que haya una como la siguiente: READ THE 22ND LOGICAL RECORD FROM THE FILE NAMED DIR1/MY/FILE.TXT (LEE EL REGISTRO LÓGICO 22 DEL ARCHIVO LLAMADO DIR1/MY/FILE.TXT).

La capa superior de abstracción no es capaz de llevar a cabo esta solicitud por sí misma. Una vez que dicha capa ha definido la dirección física del archivo mediante su nombre simbólico (DIR1/MY/FILE.TXT), envía la solicitud siguiente a la capa inferior: READ THE 22ND LOGICAL RECORD FROM THE FILE LOCATED BY THE FOLLOWING PHYSICAL ADDRESS: 174 AND HAVING THE SIZE EQUAL TO 235. (LEE EL REGISTRO LÓGICO 22 DEL ARCHIVO UBICADO EN LA SIGUIENTE DIRECCIÓN FÍSICA: 174 Y QUE TIENE UN TAMAÑO IGUAL A 235.)

Como respuesta a dicha solicitud, la segunda capa determina que el archivo con la dirección 174 ocupa cinco áreas no adyacentes del disco y que el registro requerido está ubicado en el cuarto fragmento del archivo localizado en el bloque físico 345. Después, envía la solicitud al controlador del disco con el fin de leer el registro lógico requerido.

De acuerdo con nuestro método simplificado, la interacción entre las capas del sistema de archivos era unidireccional, de la parte superior a la inferior; sin embargo, la situación real es mucho más compleja. Para determinar las características del archivo, la capa superior tiene que decodificar el nombre del archivo simbólico (es decir, leer en secuencia la trayectoria completa de directorios especificados en el nombre del archivo totalmente identificado). Lo anterior significa que la capa superior debe enviar una solicitud más de una vez a la capa que está por debajo de ella. La capa inferior deberá preguntar varias veces al controlador del disco que lea los datos de la estructura del directorio del disco físico. En cada ocasión, los resultados de las operaciones realizadas se enviarán de la parte inferior a la superior.

El problema que implica la organización de la interacción entre computadoras mediante el uso de la red puede representarse también como un conjunto de módulos organizados jerárquicamente. Por ejemplo, las tareas que aseguran la transmisión confiable de datos entre nodos vecinos pueden delegarse a los módulos de la capa inferior; a su vez, los módulos de los niveles superiores pueden encargarse del transporte de mensajes a través de toda la red. Obviamente, está última tarea —la organización de la interacción entre cualquier par de nodos, no necesariamente adyacentes— es más general. Por lo tanto, este problema puede resolverse mediante el uso de solicitudes múltiples a la capa inferior. En consecuencia, la organización de la interacción entre los nodos A y B (figura 4.4) puede reducirse a la conexión secuencial de pares de nodos de paso.

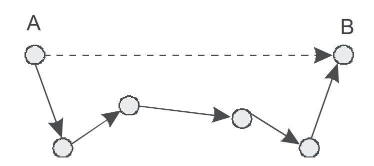


FIGURA 4.4 Conexión de un par de nodos de red.

4.2.2 Protocolo y pila de protocolos

La representación multicapa de las herramientas de red tiene características especiales, porque al menos hay *dos instancias* involucradas en el proceso de intercambio de mensajes. Esto significa que en este caso en particular es necesario organizar la operación coordinada de dos jerarquías de herramientas de red que se ejecutan en dos computadoras. Ambos participantes del intercambio de red deben estar de acuerdo en varias convenciones; por ejemplo, ambos deben estar de acuerdo en los niveles y formas de las señales eléctricas, en el método para determinar el tamaño del mensaje y los métodos de detección de errores. En otras palabras, los acuerdos tienen que hacerse en todas las capas, desde la más inferior —la de transmisión de bits— hasta la más alta, encargada de implementar los servicios para los usuarios de la red.

La figura 4.5 muestra el modelo de interacción entre dos nodos. En cada parte, las herramientas de interconexión se representan por cuatro capas, cada una de las cuales soporta dos tipos de interfases. Primero, existen interfases de servicio hacia las capas superior e inferior de la jerarquía local de herramientas de red; segundo, debe existir una interfase hacia las herramientas de interacción de la otra instancia, localizada en el mismo nivel jerárquico. Este tipo de interfase se conoce con el nombre de **protocolo**. Por lo tanto, el protocolo siempre representa una **interfase de igual a igual**.

NOTA *Básicamente, los términos protocolo e interfase significan lo mismo, es decir, se trata de descripciones formales del procedimiento de interacción entre dos objetos; sin embargo, en las redes, por tradición ambos términos tienen diferentes campos de aplicación: los protocolos definen las reglas de interacción entre módulos de la misma capa que corren o se ejecutan en nodos distintos y las interfases definen las reglas de interacción entre los módulos de capas adyacentes dentro del mismo nodo.*

Al conjunto de protocolos organizado jerárquicamente y que es suficiente para llevar a cabo la interacción entre los nodos de una red se le conoce con el nombre de **pila de protocolos** (o **conjunto de protocolos** o **suite de protocolos**).

Los protocolos de las capas inferiores a menudo se implementan como una combinación de hardware y software, en tanto que los de nivel superior sólo se implementan en software.

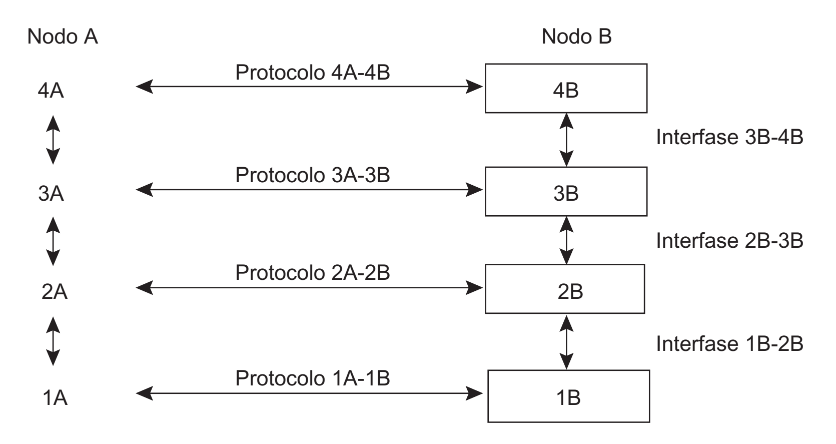


FIGURA 4.5 Interacción entre dos nodos.

Un módulo de software que cumple un protocolo específico se conoce con el nombre de **entidad del protocolo** o simplemente protocolo. El mismo protocolo puede llevarse a cabo de manera más o menos eficaz. Por esta razón, es necesario tener en cuenta la lógica de operación del protocolo y la calidad de su implementación cuando se comparan diferentes protocolos; además, *la eficacia de la interacción entre los dispositivos de red depende de la calidad del conjunto de protocolos que forman la pila de protocolos.* En particular, es necesario evaluar qué tan eficientemente están distribuidas las funciones entre los protocolos de las diversas capas y con cuánta claridad se encuentran definidas las interfases entre las capas de protocolos.

Las entidades de los protocolos de la misma capa de dos instancias que interactúan entre sí, intercambian mensajes de acuerdo con las reglas del protocolo. Por lo general, los mensajes comprenden el encabezado y el campo de datos (que en ocasiones puede dejarse en blanco). El intercambio de mensajes es un tipo de lenguaje que utilizan las instancias para *explicarse* una a otra qué debe hacerse en cada etapa de la interacción. La operación de cada módulo del protocolo consiste en interpretar los encabezados de los mensajes entrantes y realizar las acciones correspondientes. Los encabezados de los mensajes de protocolos distintos poseen estructuras diferentes que corresponden a la variedad en su funcionamiento. A medida que la estructura del encabezado del mensaje es más compleja, las funciones delegadas al protocolo correspondiente son más sofisticadas.

4.3 MODELO OSI

PALABRAS CLAVE: organización para la estandarización (ISO), sector de estandarización de las telecomunicaciones (ITU-T), interconexión de sistemas abiertos (OSI), modelo de referencia, interfase de programación de la aplicación (API), encabezado, remolque, trama, paquete, datagrama, trama, segmento, mensaje, unidad de datos del protocolo (PDU), capa física, capa de enlace de datos, capa de red, capa de transporte, capa de sesión, capa de presentación, capa de aplicación, protocolos punto a punto, secuencia de verificación de tramas (FCS), control del acceso al medio (MAC), Internet, conectividad de redes, direcciones globales o de red, ruteador, enrutamiento, tablas de enrutamiento, protocolos ruteados y de enrutamiento.

El protocolo representa un acuerdo entre dos nodos de red que interactúan entre sí; sin embargo, esto no necesariamente sirve como evidencia de que este protocolo está estandarizado. No obstante, en la práctica, los arquitectos de redes se esfuerzan en usar protocolos estándar cuando implantan redes. Dichos protocolos van de acuerdo con los estándares de los propietarios, ya sean nacionales o internacionales.

A principios de la década de 1980, varias organizaciones internacionales de estándares, en las que se incluyen la **Organización Internacional para la Estandarización (ISO)** y el **Sector de Estandarización de las Telecomunicaciones del ITU (ITU-T)**, diseñaron el **modelo de interconexión de sistemas abiertos (OSI)**. Este modelo desempeña un papel muy importante en el desarrollo de las redes de computadoras.

4.3.1 Características generales del modelo OSI

A finales de la década de 1970 existía un gran número de pilas de protocolos de propietarios de comunicaciones, ejemplo de los cuales son DECnet y la arquitectura de redes del sistema (SNA, por sus siglas para System Network Architecture). Esta variedad de herramientas de

interconexión de redes puso en claro la incompatibilidad de dispositivos que utilizan protocolos diferentes. En esa época, una de las posibles formas de superar este problema parecía consistir en la migración hacia el uso de pilas de protocolos unificados creados con el fin de compensar las desventajas de las pilas de protocolos existentes. Dicho método académico para desarrollar la nueva pila de protocolos tuvo su origen en el diseño del modelo OSI, el cual no contiene descripciones de ninguna pila de protocolos en específico pues su objetivo es diferente: proporcionar una descripción generalizada de las herramientas de interconectividad de redes. El modelo OSI fue ideado como un tipo de lenguaje universal para los especialistas en la conectividad de redes. Por esta razón, a menudo se le conoce como **modelo de referencia**. El desarrollo del modelo OSI tomó siete años (de 1977 a 1984).

El modelo OSI define lo siguiente:

- Las capas de intercomunicación de los sistemas de las redes de conmutación de paquetes
- Nombres estándar para dichas capas
- Las funciones que debe realizar cada capa

En el modelo OSI (figura 4.6), las herramientas de intercomunicación se dividen en siete capas: la de aplicación, la de presentación, la de sesión, la de transporte, la de red, la de enlace de datos y la física. Cada capa tiene que ver con un aspecto de la conectividad de redes estrictamente definido.

IMPORTANTE *El modelo OSI describe solamente herramientas del sistema implementadas por el sistema operativo, por las utilidades y por el hardware del sistema. Este modelo no incluye las herramientas para la interacción entre las aplicaciones de los usuarios. Es importante distinguir entre el nivel de interacción que se da entre las aplicaciones y la capa de aplicación del modelo OSI.*

Las aplicaciones pueden establecer sus protocolos de interacción mediante el uso del conjunto de siete capas de herramientas del sistema. Para este fin, a los programadores se les proporciona una **interfase de programación de aplicaciones (API)** especial. De acuerdo con el diseño canónico del modelo OSI, la aplicación puede enviar sus solicitudes al nivel más alto de la jerarquía: la capa de aplicación; sin embargo, en la práctica, la mayoría de las pilas de protocolos de comunicaciones facilitan a los programadores llamar directamente a los servicios de las capas inferiores.

Por ejemplo, algunos DBMS cuentan con herramientas incorporadas para el acceso remoto a archivos. En este caso, la aplicación no utiliza el servicio de archivos del sistema cuando accede al recurso remoto. En lugar de eso, se salta las capas superiores del modelo OSI y solicita directamente las herramientas del sistema responsables del transporte de mensajes, las cuales residen en las capas inferiores del modelo OSI.

Suponga que la aplicación A que se ejecuta en la computadora 1 necesita comunicarse con la aplicación B que corre en la computadora 2. Para lograr lo anterior, la aplicación A solicita un servicio de la capa de aplicación (por ejemplo, el servicio de archivos). Con base en esta solicitud, el software de la capa de aplicación forma un mensaje en el formato estándar. Sin embargo, para entregar esta información al destino, es necesario llevar a cabo algunas otras tareas, cuya responsabilidad está encomendada a las capas inferiores.

Después de formar el mensaje, la capa de aplicación lo dirige hacia la capa de presentación. El protocolo de la capa de presentación, de acuerdo con la información recibida en el **encabezado** del mensaje de la capa de aplicación, lleva a cabo las acciones requeridas y adiciona al mensaje su propia información: el encabezado de la capa de presentación. Dicho

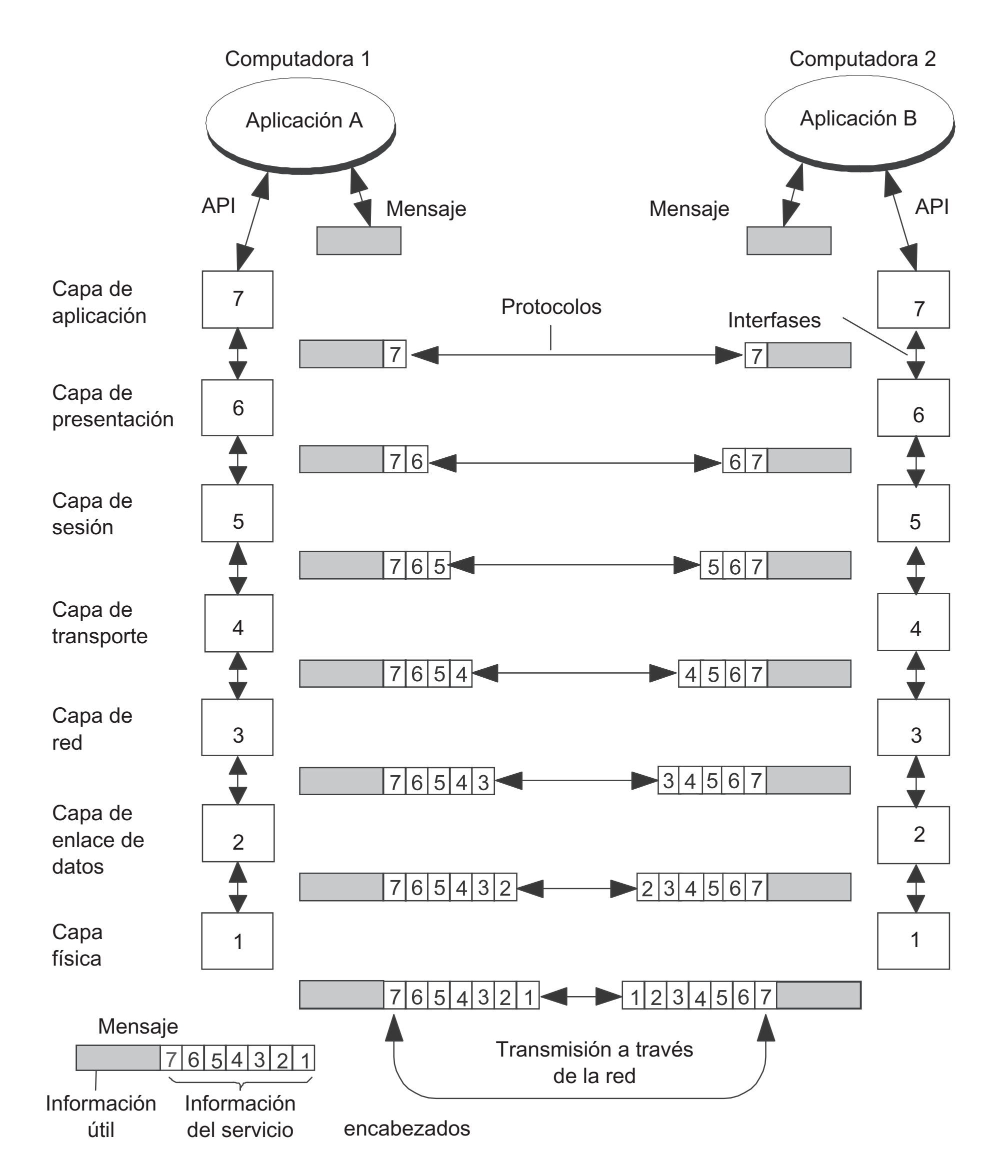


FIGURA 4.6 Modelo ISO/OSI.

encabezado contiene instrucciones para el protocolo de la capa de presentación de la máquina con la que se comunicará. El mensaje resultante es turnado posteriormente a la capa de sesión que se encuentra por debajo de ella, la que a su vez adiciona su encabezado, y así sucesivamente. Algunas implantaciones de protocolos colocan su información no sólo al comienzo del mensaje, en forma de un encabezado, sino también al final del mensaje, en el llamado **remolque**. Por último, el mensaje llega a la capa física, la cual en realidad lo envía a la máquina con la que se comunicará mediante el uso de enlaces de conexión. Para entonces, el mensaje transporta los encabezados de todas las capas (figura 4.7).

La capa física coloca el mensaje en la interfase de salida de la computadora 1, desde la cual comienza su viaje a través de la red. Observe que, hasta ese momento, el mensaje fue transferido de capa en capa dentro de la computadora 1.

Cuando el mensaje se entrega a la computadora 2 es recibido por la capa física y se transfiere secuencialmente hacia arriba capa por capa. Cada una inspecciona el encabezado de

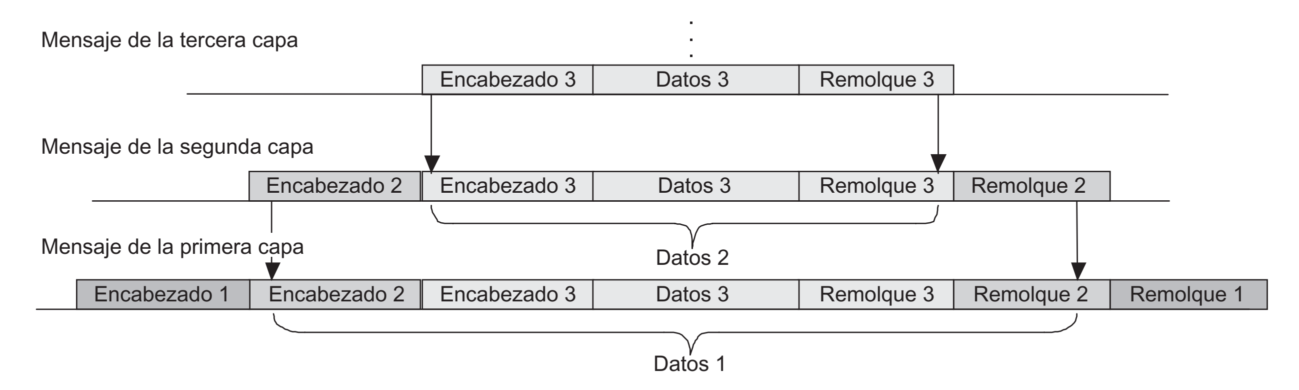


FIGURA 4.7 Anidado de los mensajes de las diferentes capas.

su propia capa, lleva a cabo las funciones que se requieran y después elimina el encabezado y pasa el mensaje a la siguiente capa.

Es evidente que las entidades del protocolo de la misma capa nunca se comunican de manera directa. Esta interacción se halla siempre mediada por las herramientas de los protocolos de las capas inferiores. Sólo las capas físicas de los diferentes nodos interactúan de forma directa.

Además del término **mensaje**, existen otros que utilizan los profesionales para representar las unidades de intercambio de datos. Entre los estándares de la ISO existe un nombre genérico para designar las unidades de intercambio de datos relacionado con los protocolos de las diferentes capas: **Unidad de Datos del Protocolo (PDU)**. Los términos especializados se utilizan a menudo para representar las unidades de intercambio de datos de las diferentes capas: **trama**, **paquete**, **datagrama** y **segmento**.

4.3.2 Capa física

La **capa física** se encarga de la transmisión de la corriente de bytes mediante el uso de enlaces físicos, como el cable coaxial, el cable de par trenzado, el cable de fibra óptica o un circuito digital de larga distancia. En el capítulo 2 ya fueron consideradas las propiedades básicas de esta capa (consulte la sección titulada "Problemas de la transmisión física de datos utilizando enlaces de comunicaciones").

Las funciones de la capa física se llevan a cabo en todos los dispositivos conectados a la red. Dentro de la computadora, las funciones de la capa física son realizadas por el adaptador de red o el puerto serial.

La especificación 10Base-T de la tecnología Ethernet puede servir como ejemplo de protocolo de capa física. Esta especificación define el par trenzado sin protección categoría 3 con una impedancia de 100 ohms como cable, un conector RJ-45, una longitud máxima de segmento de 100 metros, el código Manchester para la representación de datos en el cable y otras características del medio de transmisión y de las señales eléctricas.

A la capa física no le interesa el significado de la información que transmite. Desde este punto de vista, tal información representa un flujo uniforme de bits que deben ser entregados en su destino sin distorsiones y de acuerdo con una frecuencia de reloj específica (el intervalo predefinido entre bits adyacentes).

4.3.3 Capa de enlace de datos

La **capa de enlace de datos** es la primera (de abajo hacia arriba) que opera en modo de conmutación de paquetes. En esta capa, al PDU generalmente se le conoce como **trama**.

Tanto en las LAN como en las WAN, las funciones de la capa de enlace de datos se definen de forma diferente. Cuando el modelo OSI estaba en construcción, las tecnologías LAN y WAN eran tan distintas que fue imposible generalizar sus operaciones de manera incondicional. Por lo tanto, las herramientas de la capa de enlace de datos deben proporcionar las funciones siguientes:

- **En las LAN**: asegurar la entrega de tramas entre *cualquier* par de nodos de la red. Se supone que la red tiene una topología típica, como un bus común, anillo, estrella o árbol (estrella jerárquica). Algunos ejemplos de redes cuyo uso está limitado a las topologías estándar incluyen Ethernet, FDDI y *Token Ring*.
- **En las WAN**: asegurar la entrega de tramas sólo entre dos nodos *vecinos* conectados mediante enlaces de comunicaciones independientes. Ejemplos de **protocolos punto a punto** (como a menudo se llama a dichos protocolos) incluyen aquellos ampliamente conocidos como el PPP y el HDLC. Es posible construir redes de cualquier topología con base en los enlaces punto a punto.

Para interconectar LAN o asegurar la entrega de mensajes entre cualquier par de nodos en una WAN, es necesario utilizar herramientas de conectividad de redes de una capa superior.

Una de las funciones que desempeña la capa de enlace de datos es *soportar las interfases* hacia la capa física inferior y hacia la capa superior siguiente (capa de red). La capa de red envía los paquetes que deben ser transmitidos utilizando la red, hacia la capa de enlace de datos y recibe de ésta paquetes que llegan desde la red. La capa de enlace de datos usa la capa física como una herramienta que recibe una secuencia de bits de la red o transmite la secuencia de bits hacia ésta.

Considere la forma como opera la capa de enlace de datos, a partir del momento en el que la capa de red del emisor se dirige a la capa de enlace de datos y le envía un paquete con la dirección del nodo de destino. Para llevar a cabo esta función, la capa de enlace de datos genera una trama que incluye el campo de datos y el encabezado. La capa de enlace de datos encapsula el paquete en el campo de datos de la trama y llena el encabezado de la trama con la información apropiada acerca del servicio. La dirección de destino que utilizarán los interruptores de red para el envío de paquetes es la información más importante del encabezado de la trama.

Otra de las tareas de la capa de enlace de datos es la *detección y corrección de errores*. Para lograr estas funciones, la capa de enlace de datos limita las fronteras de la trama colocando una secuencia especial de bits tanto a su comienzo como en su final. Posteriormente, la capa de enlace de datos agrega una suma verificadora especial a la trama, también conocida con el nombre de **secuencia de verificación de tramas (FCS)**. La suma verificadora se calcula de acuerdo con cierto algoritmo en función del número total de bytes que conforman la trama. Mediante el uso del valor del campo FCS, el nodo de destino podrá determinar si los datos de la trama sufrieron algún daño durante la transmisión a través de la red.

Sin embargo, antes de transferir la trama a la capa física para su transmisión a través de la red, la capa de enlace de datos deberá resolver otro problema importante. Si la red utiliza un medio de transmisión compartido, antes de que la capa física empiece la transmisión de datos, la capa de enlace de datos tendrá que *verificar la disponibilidad del medio de transmisión* (cuando no se utiliza un medio de transmisión compartido, se omite dicha

verificación). Las funciones que llevan a cabo la verificación de la disponibilidad del medio compartido se clasifican a menudo como una subcapa independiente, llamada **control de acceso al medio (MAC)**.

Si el medio compartido está libre, la trama será transferida a la red por la capa física, la cual viaja utilizando los enlaces de comunicaciones y llega a la capa física del nodo de destino en forma de una secuencia de bits. Esta capa, a su vez, transfiere los bits recibidos *hacia arriba* a la capa de enlace de datos en el nodo de destino. Esta última capa agrupa los bits en tramas, recalcula la suma verificadora de los datos recibidos y compara el resultado con la suma verificadora de la trama. Si ambos valores coinciden, la trama se considerará correcta; si no coinciden, se reportará la presencia de un error. Las funciones de la capa de enlace de datos incluyen tanto la detección como la corrección de errores al retransmitir las tramas dañadas; sin embargo, esta función no es obligatoria. Algunas implementaciones de la capa de enlace de datos, como Ethernet, *Token Ring*, FDDI y *Frame Relay*, carecen de esta función.

Los protocolos de la capa de enlace de datos están implementados en computadoras, puentes, interruptores y ruteadores. En las computadoras, las funciones de la capa de enlace de datos se cumplen gracias a la operación coordinada de los adaptadores de red y sus controladores.

El protocolo de la capa de enlace de datos por lo regular opera dentro de una red que representa un fragmento de una red más grande, unida mediante los protocolos de una capa de red. Las direcciones de la capa de enlace de datos se utilizan para la entrega de tramas sólo dentro de una red, mientras que las direcciones de la capa superior (capa de red) se usan para el envío de paquetes entre redes.

En las LAN la capa de enlace de datos representa un conjunto completo y poderoso de funciones para la transmisión de mensajes entre los nodos de la red. En algunos casos, los protocolos de la capa de enlace de datos de la LAN son herramientas de transporte autosuficientes y permiten que los protocolos de la capa de aplicación o aplicaciones operen directamente sobre ellos. En este caso, no hay necesidad de emplear las herramientas de la capa de red o de la capa de transporte. No obstante, si se quiere asegurar una alta calidad en la transmisión de mensajes en las redes con topología arbitraria, las funciones de la capa de enlace de datos no son suficientes. Este enunciado es aún más válido en las WAN, donde los protocolos de la capa de enlace de datos realizan la simple función de la transmisión de datos entre los nodos vecinos más cercanos. En el modelo OSI, estas funciones se delegan a las dos capas superiores siguientes: la de red y la de transporte.

4.3.4 Capa de red

La **capa de red** genera un sistema de transporte unificado que conecta varias redes, también conocido como **interred** o, de manera abreviada, **Internet**. Es importante no confundir los términos *internet* e *Internet*. Esta última es la implementación mejor conocida de la interred construida con base en la tecnología TCP/IP y que abarca todo el mundo.

> La tecnología para la conexión de un gran número de redes —que en general están diseñadas con diferentes tecnologías—, en una sola red se llama **interred**.

La figura 4.8 muestra varias redes, cada una de las cuales utiliza una tecnología específica de enlace de datos: Ethernet, FDDI, *Token Ring*, ATM y *Frame Relay*. Con base en estas tecnologías, cada una de dichas redes puede conectar cualquier par de usuarios dentro de

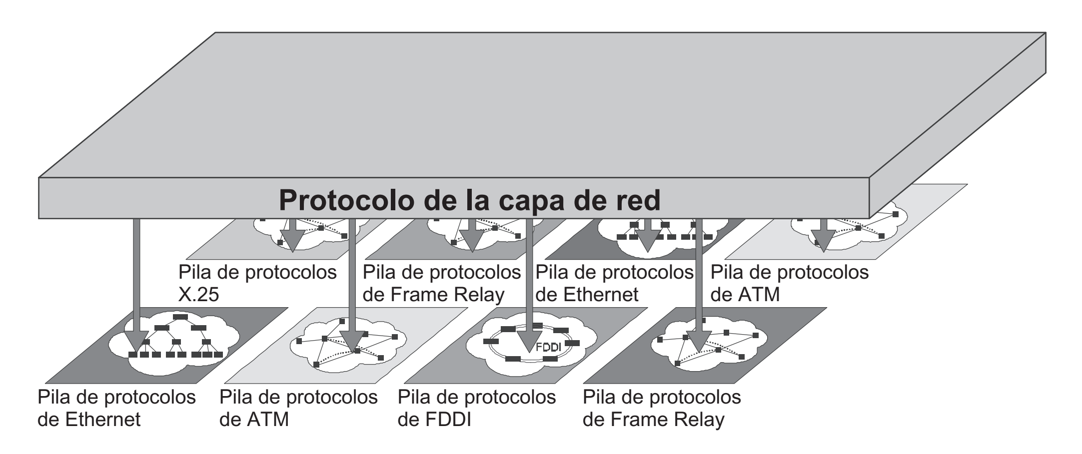


FIGURA 4.8 Necesidad de la capa de red.

una red local; sin embargo, una red no puede asegurar la transmisión de datos hacia otra red. La razón de lo anterior es evidente: las diferencias significativas de las tecnologías de red. Aun las tecnologías de LAN más parecidas —Ethernet, FDDI y *Token Ring*— que usan el mismo sistema de direccionamiento (direcciones de la subcapa MAC, conocidas como direcciones MAC), tienen distintos formatos de trama y una lógica diferente para la operación del protocolo. Las tecnologías LAN y WAN tienen aún más diferencias. La mayoría de las tecnologías WAN utilizan la técnica de establecer con antelación circuitos virtuales, cuyos identificadores se usan como direcciones. Todas las tecnologías emplean formatos de trama específicos. La trama de ATM incluso tiene un término específico para denotar este formato: **celda**. Ciertamente, todos tienen sus propias pilas de protocolos.

Para conectar redes que estén basadas en dichas tecnologías disímiles, *se requieren herramientas adicionales*. La capa de red del modelo OSI es la que proporciona dichas herramientas.

Las funciones de la capa de red se implementan por medio de lo siguiente:

- Grupo de protocolos
- Dispositivos especiales conocidos como *ruteadores*

Una de las funciones de un **ruteador** es asegurar la *conexión física de redes diferentes*. Éste cuenta con varias interfases de red similares a las de una computadora, cada una de las cuales puede conectarse a una red. Por lo tanto, todas las interfases de un ruteador pueden considerarse nodos de redes distintas. Los ruteadores pueden implementarse como un módulo de software con base en una computadora universal; por ejemplo, la configuración típica de UNIX o Windows incluye un ruteador de software. Sin embargo, muy a menudo, los ruteadores se implementan a partir de plataformas especializadas de hardware. El software del ruteador incluye entidades de los protocolos de la capa de red.

De lo anterior se infiere que para interconectar las redes que se muestran en la figura 4.8 es necesario conectar todas ellas mediante ruteadores e instalar entidades de los protocolos de la capa de red en todas las computadoras de los usuarios terminales que necesiten comunicarse empleando la interred (figura 4.9).

Los datos que deben transmitirse utilizando la interred llegan a la capa de red provenientes de la capa de transporte, después de lo cual son complementados por el encabezado de la capa de red. Los datos junto con el encabezado forman un *paquete*: el término común para denotar el PDU de la capa de red. El encabezado del paquete de la capa de red tiene

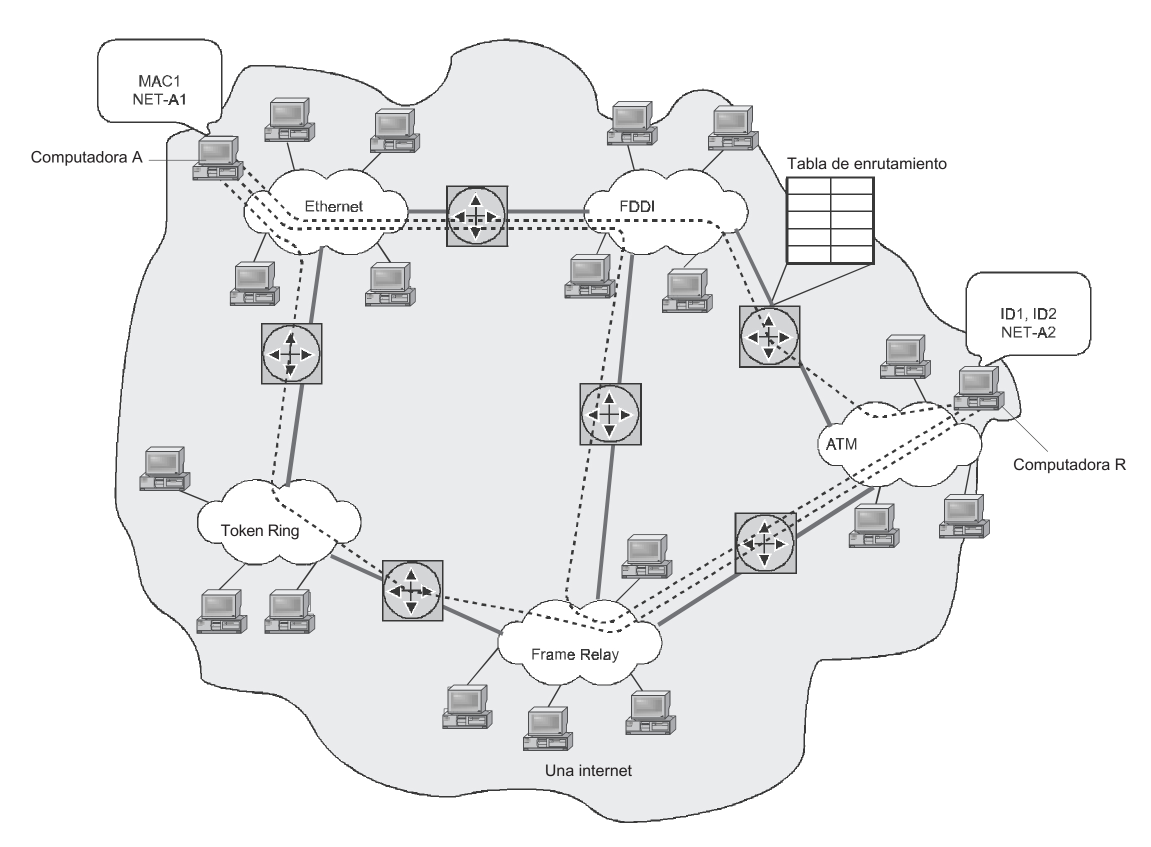


FIGURA 4.9 Ejemplo de una interred.

un formato unificado, el cual no depende de los formatos de las tramas de la capa de enlace de datos, los cuales son específicos para las redes que puedan ser parte de la interred. Este encabezado contiene la dirección de destino de este paquete, además de otra información.

Para asegurar que los protocolos de la capa de red puedan entregar paquetes a cualquier nodo de la interred, es necesario asegurar que cada nodo tenga una dirección que sea única dentro de los límites de esta interred. Dichas direcciones se conocen con el nombre de **direcciones de red** o **direcciones globales**. Cada nodo de la interred que tenga que intercambiar datos con los demás nodos de internet debe contar con una dirección de red, junto con la dirección que la tecnología de la capa de enlace de datos le haya asignado. Por ejemplo, en la figura 4.9, una computadora de una red Ethernet, que a su vez está dentro de una interred, tiene la dirección de la capa de enlace de datos *MAC1* y la dirección de la capa de red *NET-A1.* De manera similar, el nodo de la red ATM direccionado por los identificadores de circuitos virtuales *ID1* e *ID2* tiene la dirección de red *NET-A2*. El paquete de la capa de red debe especificar la dirección de la capa de red como una dirección de destino. La ruta del paquete estará determinada con base en esta dirección.

El **enrutamiento** representa una tarea importante de la capa de red. La ruta se describe mediante una secuencia de redes (o ruteadores) a través de las que el paquete debe viajar para ser entregado al nodo de destino. La figura 4.9 muestra tres rutas por las cuales los datos pueden transmitirse de la computadora A a la B. El ruteador recaba información acerca de la topología de los enlaces de la interred y crea tablas de conmutación con base en esta topología. Observe que en este caso, dichas tablas de conmutación tienen un nombre especial: **tablas de enrutamiento**. La tarea de seleccionar una ruta se explicó de manera breve en el capítulo 2 (consulte la sección "*Problema generalizado de la conmutación*").

De acuerdo con el método multicapas, la capa de red solicita a la capa de enlace de datos que está debajo de ella que realice sus funciones. Toda la trayectoria a través de la interred se divide en secciones, cada una de las cuales corresponde a la trayectoria a través de la red específica, de un ruteador al otro.

Para transmitir el paquete a través de la siguiente red, la capa de red coloca el paquete en el campo de datos de la trama correspondiente a una tecnología específica de enlace de datos y determina la dirección de la capa de enlace de datos de la interfase del ruteador siguiente. La red, por medio de la tecnología de enlace de datos apropiada, entrega la trama con su paquete encapsulado usando la dirección especificada. El ruteador copia el paquete de la trama entregada, lo procesa y después lo pasa a la red siguiente para su futuro transporte. Antes de hacer eso, el ruteador debe encapsular el paquete en la nueva trama de enlace de datos. Dicha trama debe tener un formato diferente en función de la tecnología utilizada. Por lo tanto, la capa de red desempeña el papel de coordinador y organiza la operación coordinada de las redes basadas en tecnologías disímiles.

EJEMPLO *La operación de la capa de red es, de alguna forma, similar a la de un servicio de mensajería internacional, como DHL o TNT (figura 4.10). Suponga que es necesario transportar ciertos artículos de la ciudad A a la B, las cuales están ubicadas en diversos continentes. Para la entrega de los artículos, la empresa de mensajería internacional puede usar los servicios proporcionados por los diferentes proveedores de servicio regionales, entre los que se incluyen:*

- *Ferrocarril*
- *Transporte marítimo*
- *Compañías aéreas*
- *Transporte motorizado*

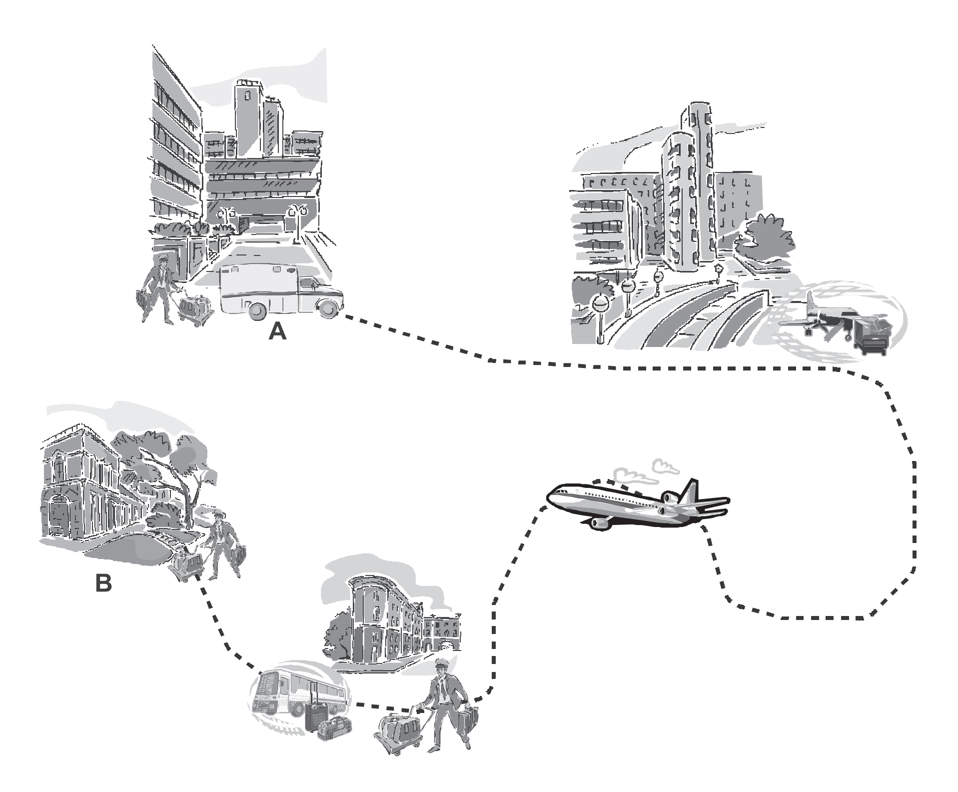


FIGURA 4.10 Funcionamiento del servicio postal internacional.

Dichas compañías pueden ser consideradas análogas a la capa de enlace de datos de las redes, y cada red es construida con base en una tecnología específica. El servicio de mensajería internacional debe organizar la red unificada y bien coordinada a partir de estos proveedores regionales del servicio. Para ello, en primera instancia, debe planear la ruta para el transporte de los bienes y, después, coordinar la operación en los puntos donde cambian los proveedores regionales del servicio. Esto puede ser, por ejemplo, la descarga de la mercancía de un automóvil. El cargamento es, posteriormente, colocado en el compartimiento de carga de un avión. Cada proveedor del servicio de transporte es responsable de llevar los bienes a través de su trayectoria asignada dentro de la ruta, pero no de las condiciones o del transporte de los bienes fuera de su sección.

En general, las funciones de la capa de red son más que simplemente asegurar el intercambio de datos dentro de la interred. Por ejemplo, la capa de red resuelve el problema de crear barreras confiables y flexibles para las trayectorias con tráfico indeseable entre redes.

Para finalizar la descripción de la capa de red, permítanos mencionar que en esta capa existen dos tipos de protocolos. Los **protocolos ruteados** *representan el primer tipo de protocolos que se encargan del envío de paquetes a través de la red.* Éstos son los protocolos a los que uno por lo general se refiere cuando se estudian los protocolos de la capa de red; sin embargo, existen otro tipo de protocolos: los **protocolos de enrutamiento**, *que a menudo se clasifican como protocolos de la capa de red.* Por medio de estos últimos, los ruteadores recaban información acerca de la topología de los enlaces de la interred, con base en la ruta seleccionada para el envío de paquetes.

4.3.5 Capa de transporte

Los paquetes pueden perderse o dañarse a lo largo de su camino desde el emisor al receptor. Aunque algunas aplicaciones cuentan con herramientas para el manejo de errores, existen otras aplicaciones que, en principio, prefieren trabajar con conexiones confiables.

La **capa de transporte** proporciona aplicaciones a las capas superiores del modelo OSI —las capas de aplicación, presentación y sesión— por medio del servicio de la transmisión de datos con el nivel de confiabilidad requerido. El modelo OSI define cinco clases de servicio de transporte, comenzando por la clase 0 (la más baja) hasta la clase 4 (la más alta). Estas clases difieren en la calidad de los servicios que proporcionan: la urgencia, la posibilidad de restablecer conexiones rotas, la disponibilidad de las herramientas para el multiplexaje de varias conexiones entre los diferentes protocolos de la capa de aplicación mediante un protocolo común de transporte y, lo más importante, la capacidad para detectar y corregir los errores en la transmisión, como la distorsión de datos, la pérdida de paquetes o la duplicación.

Por un lado, la selección de la clase de servicio de capa de transporte depende del grado en que el problema del aseguramiento de la confiabilidad sea resuelto por las aplicaciones y protocolos de las capas que están más arriba de la capa de transporte. Por otro lado, esta selección depende de la confiabilidad del sistema de transporte de datos de la red, la cual está asegurada por las capas que se hallan por debajo de la capa de transporte: las capas de red, de enlace de datos y física. Por ejemplo, si la calidad de los enlaces de comunicaciones es elevada y la probabilidad de la presencia de errores que no puedan ser detectados por los protocolos de las capas inferiores es baja, tendrá sentido utilizar uno de los servicios ligeros de la capa de transporte, los cuales no se saturan por las verificaciones múltiples, los reconocimientos de recepción y por otras técnicas para incrementar la confiabilidad. Si las herramientas de transporte de las capas inferiores no son lo suficientemente confiables,

tendrá sentido utilizar los servicios más avanzados de la capa de transporte, los cuales usan el máximo número posible de herramientas para la detección y corrección de errores, incluidos el establecimiento de la conexión lógica, el control de la entrega del mensaje mediante sumas verificadoras y la numeración cíclica de paquetes, así como el establecimiento de los tiempos máximos de entrega.

Todos los protocolos de la capa de transporte y mayores se implementan gracias a herramientas de software instaladas en los nodos terminales de la red: son componentes de sus sistemas operativos de red. Algunos ejemplos de protocolos de transporte son el TCP y el UDP de la pila TCP/IP y el protocolo SPX de la pila de protocolos de Novell.

Los protocolos de las cuatro capas inferiores se conocen como **transporte de la red** o **subsistema de transporte**, ya que éstos resuelven el problema del transporte de mensajes con un nivel de calidad específico, en las redes que utilizan una topología arbitraria con base en diferentes tecnologías. Tres capas superiores resuelven los problemas de brindar los servicios de aplicación mediante el uso del subsistema de transporte.

4.3.6 Capa de sesión

La **capa de sesión** asegura el control de las interacciones entre instancias. Esta capa registra la instancia activa y proporciona las herramientas necesarias para sincronizar la sesión. Dichas herramientas posibilitan la inserción de puntos de verificación en transmisiones largas con el fin de asegurar que, en caso de una falla, haya un regreso sin problemas al último punto de verificación, en vez de volver a comenzar todo desde el principio. En la práctica las aplicaciones que utilizan la capa de sesión no son muy numerosas. Esta capa rara vez se implementa en la forma de entidad de protocolo independiente. Con mucha frecuencia, las funciones de esta capa se combinan con las de la capa de aplicación y ambas se implementan como un solo protocolo.

4.3.7 Capa de presentación

La **capa de presentación** se encarga de la forma como se presenta la información transmitida a través de la red, sin cambiar su contenido. Gracias a esta capa, la información transmitida por la capa de aplicación de un sistema es siempre comprensible por la capa de aplicación de otro sistema. Mediante el uso de las herramientas de esta capa, los protocolos de la capa de aplicación pueden superar los errores de sintaxis en la presentación de los datos o las diferencias que existen entre los códigos de caracteres, como los códigos ASCII y EBCDIC. En esta capa se realizan las tareas de encriptado y desencriptado de datos, las cuales aseguran el intercambio confiable de datos para todos los servicios de aplicación. Un ejemplo de dicho protocolo es la capa de conexión segura (Secure Socket Layer, SSL), que asegura el intercambio confiable de mensajes de los protocolos de la capa de aplicación de la pila de protocolos TCP/IP.

4.3.8 Capa de aplicación

La **capa de aplicación** es, en realidad, un conjunto de protocolos que los usuarios de la red emplean para acceder a los recursos compartidos de la red, como archivos, impresoras o páginas web. Dichos protocolos pueden también trabajar en grupo mediante el uso, por ejemplo, de protocolos de correo electrónico. La unidad de datos con las que trabaja la capa de aplicación generalmente se conoce con el nombre de **mensaje**.

Existen muchos servicios de la capa de aplicación. Algunos ejemplos de las implantaciones más conocidas de servicios de archivos de red son el NFS y el FTP en la pila TCP/IP, SMB de Windows de Microsoft y el NCP de Novell NetWare.

En la capa de aplicación es donde se encuentran las aplicaciones interesantes que realizan trabajo para el usuario final; esta capa requiere de protocolos de apoyo, como es el caso del DNS (Sistema de nombres de dominios), que permite referirse a direcciones IP mediante nombres. En teoría, un DNS puede estar ubicado en un solo servidor, conocido como "servidor de nombres".

Otra aplicación importante es el correo electrónico o e-mail, que es un sistema de comunicación asíncrono entre usuarios.

Sin duda otra de las grandes e interesantes aplicaciones es la World Wide Web (conocida como WWW), que es una estructura arquitectónica para tener acceso a documentos vinculados de manera distribuida sobre Internet. Así, desde el punto de vista del usuario, la WWW consiste en un enorme conjunto de documentos a nivel mundial que se conoce como páginas web, las cuales pueden tener vínculos a otras páginas web; a esto se le conoce como hipertexto. Las páginas web pueden ser visualizadas mediante un "navegador", como por ejemplo el Internet Explorer.

Otra gran aplicación es la "Voz sobre IP", que consiste en utilizar la red de datos para transmitir la voz de manera digitalizada como datos y así poder utilizar incluso Internet para establecer llamadas por la red de redes como si se enviaran datos. Los protocolos usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de voz sobre IP, o protocolos IP. Pueden ser vistos como implementaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET. La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN). Algunos ahorros en el costo se deben a la utilización de una misma red para llevar voz y datos, especialmente cuando los usuarios no utilizan toda la capacidad de una red ya existente en la cual pueden usar VoIP sin un costo adicional. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VoIP a PSTN, que generalmente cuestan al usuario de VoIP.

4.3.9 Modelo OSI y redes de conmutación de circuitos

Como ya se mencionó, el modelo OSI describe el proceso de interacción entre dispositivos de una *red de conmutación de paquetes*. ¿Y qué hay respecto a las *redes de conmutación de circuitos*?, ¿existe algún modelo de referencia para dichas redes?, ¿es posible comparar las funciones de las tecnologías de conmutación de circuitos con las capas del modelo OSI?

Las herramientas para la conectividad de redes para las redes de conmutación de circuitos también se pueden representar mediante el uso de un método multicapa, lo cual depende de cuáles sean las capas de protocolos que formen la jerarquía. Sin embargo, en las redes de conmutación de circuitos, no existe un modelo de referencia similar al modelo OSI. Por ejemplo, los diferentes tipos de redes telefónicas utilizan pilas de protocolos específicos de la red, y éstas difieren en el número de capas y la distribución de funciones entre ellas. Las redes de transmisión, como la jerarquía digital sincrónica (SDH) y el multiplexaje denso por división de longitud de onda (DWDM), también tienen su jerarquía de protocolos. La situación es todavía más compleja, ya que las redes más modernas de este tipo utilizan redes de conmutación de circuitos para solamente transmitir los datos de usuario. Para controlar los procesos del establecimiento de la llamada y la administración general de la red, se emplea

la técnica de conmutación de paquetes. Por ejemplo, SDH, DWDM y las redes telefónicas modernas utilizan este método.

A pesar de que las redes de conmutación de circuitos cuentan con una organización sofisticada y soportan su propia jerarquía de protocolos, éstas proporcionan el servicio de la capa física a las redes de conmutación de paquetes.

Como ejemplo, considere varias LAN de conmutación de paquetes interconectadas mediante el uso de una red telefónica digital. Como es evidente, las funciones de conectividad de redes se delegan a los protocolos de la capa de red, lo cual hace necesario instalar un ruteador en cada LAN. El ruteador debe estar equipado con una interfase capaz de establecer conexiones con otra LAN que utilice una red telefónica. Cuando se establece dicha conexión se genera un flujo de bits con velocidad constante en la red telefónica; esta conexión proporcionará el servicio de la capa física a los ruteadores. Con el fin de organizar la transmisión de datos, los ruteadores usan un protocolo punto-a-punto de la capa de enlace de datos en este circuito.

4.4 ESTANDARIZACIÓN DE REDES

PALABRAS CLAVE: sistema abierto, especificación, especificaciones abiertas, estándares propietarios, estándares de comités especiales, estándares nacionales, estándares internacionales, Solicitudes de Comentarios (RFC), Sociedad de Internet (ISOC), Consejo de la Arquitectura de Internet (IAB), Fuerza de Tarea de la Investigación acerca de Internet (IRTF), Fuerza de Tarea de la Ingeniería de Internet (IETF), modelo OSI, pila de protocolos de OSI, pila IPX/SPX, pila NetBIOS/SMB, pila TCP/IP, flujo, segmento y trama.

Una afirmación sobre las ventajas de la estandarización que es válida para la mayoría de las tecnologías tiene un significado especial en las redes de computadoras. La idea principal en que se apoyan las redes consiste en asegurar la comunicación entre distintos tipos de equipo. En consecuencia, uno de los problemas más urgentes e importantes es la compatibilidad. No hubiera habido ningún progreso en el campo de la conectividad de redes sin la aceptación de algunos estándares de los equipos, así como también protocolos. Debido a lo anterior, la evolución total de la industria de la computación se refleja en los estándares. Cualquier tecnología novedosa se considera *oficialmente* aceptada sólo cuando se expresa mediante el estándar o los estándares apropiados.

El modelo OSI que se estudió con anterioridad representa una base ideológica para la estandarización de las redes de computadoras.

4.4.1 Concepto de sistema abierto

¿Qué es un sistema abierto?

En un sentido amplio, un **sistema abierto** es cualquier sistema (ya sea una computadora independiente, una red de computadoras, un sistema operativo, un software de aplicación o cualquier otro hardware y software) diseñado de acuerdo con especificaciones abiertas.

Recuerde que el término **especificación** en el campo de la computación significa una descripción formalizada de componentes de hardware o software, los métodos para su operación, su interacción con otros componentes, las condiciones de operación y otras características especiales. Como es obvio, no toda especificación es un estándar.

Las **especificaciones abiertas** se publican, están disponibles y cumplen con los estándares acordados después de un estudio minucioso y variado que incluya a todas las instancias interesadas.

El uso de las especificaciones abiertas en la creación de un sistema permite que terceras instancias desarrollen diferentes extensiones de hardware y software, así como modificaciones de ese sistema. Asimismo, facilita que los integradores de sistemas puedan combinar productos de hardware o software de diversos fabricantes.

La naturaleza abierta de los estándares y las especificaciones es importante no solamente para los protocolos de comunicaciones, sino también para todos los dispositivos de hardware y productos de software utilizados cuando se construyen las redes. La mayoría de los estándares que se usan actualmente son abiertos. Los tiempos de los sistemas propietarios, los cuales eran especificaciones exactas solamente conocidas por sus respectivos fabricantes, terminaron hace mucho tiempo. Todo mundo parece haberse dado cuenta de que la capacidad de una interacción ágil y sencilla con los productos de la competencia no reduce el valor de un producto. Por el contrario, el valor del producto se incrementa significativamente, ya que dichos productos pueden emplearse en redes heterogéneas construidas con base en productos de diferentes proveedores. Por lo tanto, aun las compañías que alguna vez fabricaron sistemas propietarios como IBM, Novell y Microsoft, ahora participan activamente en el desarrollo de estándares abiertos, implantándolos en sus productos.

Desafortunadamente, en sistemas reales, una apertura total todavía representa un ideal no alcanzable. En general, incluso en los sistemas llamados abiertos, solamente las partes específicas que soportan interfases externas son abiertas en realidad. Por ejemplo, las características abiertas de la familia de sistemas operativos UNIX incluyen la disponibilidad de una interfase de software estándar entre el kernel del sistema operativo y las aplicaciones, lo cual hace posible transportar fácilmente las aplicaciones de una versión de UNIX al ambiente de otra versión.

El modelo OSI se relaciona con un solo aspecto de la apertura, es decir, con la que se necesita para la interacción entre dispositivos conectados a una red de computadoras. Aquí, el sistema abierto es interpretado como un dispositivo de red listo para interactuar con otros dispositivos de la red mediante el uso de reglas estándar que definen el formato, el contenido y los significados de los mensajes que se envían y que se reciben.

Si se diseñan dos redes de acuerdo con los principios de los sistemas abiertos se tienen las ventajas siguientes:

- La posibilidad de construir una red con base en hardware y software de diversos fabricantes que soporten el mismo estándar.
- La posibilidad de reemplazar componentes específicos de la red por unos más avanzados, lo cual permite que la red pueda actualizarse sin que esto represente un gran costo.
- La posibilidad de interconectar las redes de una manera sencilla.
- Mantenimiento de la red fácil y simple.

4.4.2 Tipos de estándares

Las actividades de estandarización de las redes de computadoras son dirigidas por varias organizaciones. En función del estatus de la organización, los estándares se clasifican como sigue:

- **Estándares propietarios:** a*lgunos de estos son la pila de protocolos* SNA, que es propiedad de IBM, y la interfase gráfica OPEN LOOK de los sistemas UNIX, que son propiedad de Sun Microsystems.
- **Estándares de comités especiales:** se crearon mediante la cooperación de varias compañías, por ejemplo, los estándares de la tecnología ATM, diseñada por el foro del mismo nombre que fue creado especialmente para eso, el cual incluye a más de 100 compañías participantes; o bien los estándares de la Alianza Fast Ethernet para las redes Ethernet a 100 Mbps.
- **Estándares nacionales:** *incluyen* FDDI, uno de los múltiples estándares diseñados por el Instituto Nacional de Estándares Americanos (ANSI) y los estándares de seguridad de los sistemas operativos ideados por el Centro Nacional de Seguridad de Cómputo (NCSC) del Departamento de Defensa de Estados Unidos.
- **Estándares internacionales:** algunos ejemplos son el modelo OSI y la pila de protocolos de comunicaciones diseñados por el ISO y numerosos estándares del ITU, incluidos los estándares de las redes X.25, *Frame Relay*, ISDN y de los módem.

Algunos estándares pueden ir ascendiendo categoría por categoría en el curso de su evolución. Por ejemplo, los estándares propietarios de productos que son populares y se utilizan ampliamente suelen convertirse en estándares internacionales *de facto*, ya que los fabricantes de todo el mundo están obligados a seguir dichos estándares para asegurar la compatibilidad de sus productos. Por ejemplo, debido al enorme éxito de la PC de IBM, el estándar propietario de su arquitectura se convirtió en el estándar internacional *de facto*.

Además, debido a su popularidad, algunos estándares propietarios que han tenido mucha difusión se han convertido en la base de los estándares *de jure* tanto nacionales como internacionales. Por ejemplo, el estándar Ethernet inicialmente diseñado por Digital Equipment, Intel y Xerox, después de algún tiempo fue adoptado como el estándar nacional IEEE 802.3, en una forma ligeramente modificada. Después, el ISO lo aprobó como el estándar internacional ISO 8802.3.

4.4.3 Estandarización en Internet

Internet es el mejor ejemplo de un sistema abierto. Dicha red evolucionó de acuerdo con los requerimientos de los sistemas abiertos. Miles de profesionales de las tecnologías de la infomación —usuarios de esta red en varias universidades, centros de investigación científica y fabricantes de hardware y software de todo el mundo— participaron en el desarrollo de estándares de esta red. Los estándares que definen la operación de Internet se conocen como **Solicitudes de Comentarios (RFC)**. Este nombre hace énfasis en la naturaleza pública y abierta de los estándares que se adoptan. Como consecuencia, Internet ha tenido mucho éxito en conectar diferentes equipos y software de un gran número de redes ubicadas alrededor del mundo.

Debido al crecimiento constante y enorme en la popularidad de Internet, los RFC se convirtieron en estándares internacionales *de facto*. Posteriormente, la mayoría de ellos obtuvieron el estatus de estándares oficiales a nivel internacional, generalmente como resultado de la aprobación por una de las organizaciones mencionadas con anterioridad (como regla, por la ISO o la ITU-T).

Algunos departamentos organizacionales son responsables del desarrollo, en particular, de la estandarización de la arquitectura y los protocolos de Internet. El papel más importante le corresponde a la **Sociedad de Internet (ISOC)**, una comunidad científica y adminis-

trativa de alrededor de 100 000 personas, la cual tiene como objetivo estudiar los aspectos comunes de la evolución de Internet, así como los problemas sociales, políticos y técnicos relacionados. La ISOC coordina el trabajo del **Consejo de la Arquitectura de Internet (IAB)**, organización cuyo ámbito abarca la coordinación de la investigación y desarrollo del la pila de protocolos TCP/IP. Esta organización representa a la autoridad principal en la aprobación de nuevos estándares de Internet.

El IAB comprende dos grupos principales: la **Fuerza de Trabajo de Investigación acerca de Internet (IRTF)** y la **Fuerza de Tarea de la Ingeniería de Internet (IETF)**. El IRTF coordina proyectos de investigación a largo plazo relacionados con el TCP/IP. Por su parte, el IETF representa al grupo de ingeniería encargado de resolver los problemas técnicos actuales de Internet; además, este grupo define especificaciones, las cuales se convierten luego en los estándares de Internet. El proceso de desarrollo y aprobación de un estándar de Internet implica ciertas etapas obligadas.

De acuerdo con el principio de apertura de Internet, todos los RFC se encuentran disponibles sin costo alguno. La lista de todos los documentos se puede encontrar en el sitio de edición de los RFC: http://www.rfc-editor.org. Cualquier RFC puede descargarse de la red sin costo alguno, lo cual está en contraste con, por citar un ejemplo, los estándares de la ISO.

4.4.4 Pilas estándares de protocolos de comunicaciones

La tendencia más importante de la estandarización en el campo de las redes de comunicaciones es la estandarización de los protocolos de comunicaciones. Las pilas de protocolos mejor conocidas son OSI, TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet y SNA, aunque no todas éstas se encuentran en uso en la actualidad.

Pila de protocolos OSI

Es necesario distinguir claramente entre el **modelo OSI** y la **pila de protocolos OSI**. En contraste con el modelo OSI, que es un método conceptual de interacción entre los sistemas abiertos, la pila de protocolos OSI es un conjunto de especificaciones para protocolos específicos.

A diferencia de otras pilas de protocolos, el OSI (figura 4.11) cumple totalmente con el modelo OSI e incluye especificaciones de protocolos en las siete capas de interacción definidas en este modelo. Esto no es una sorpresa; los diseñadores de esta pila de protocolos utilizaron el modelo OSI como referencia y como guía de acción.

Los protocolos de la pila OSI se caracterizan por tener especificaciones sofisticadas y ambiguas. Sus propiedades representan una consecuencia de la política de los diseñadores de la pila de protocolos, quienes trataron de tener en cuenta la gran variedad de las tecnologías emergentes y existentes.

A nivel de las capas física y de enlace de datos, la pila de protocolos OSI soporta protocolos como Ethernet, *Token Ring* y FDDI, así como LLC, X.25 e ISDN. En otras palabras, utiliza los protocolos de las capas inferiores desarrollados fuera de la estructura de la pila. En este aspecto, es similar a la mayoría de las demás pilas de protocolos.

Los servicios de las capas de red, transporte y sesión también están presentes en la pila de protocolos OSI, aunque en la práctica se utilizan muy rara vez. En la capa de red se pueden usar tanto el protocolo de red orientado a la conexión (CONP) como el protocolo de red no orientado a la conexión (CLNP). Con estos protocolos, se emplean los dos protocolos

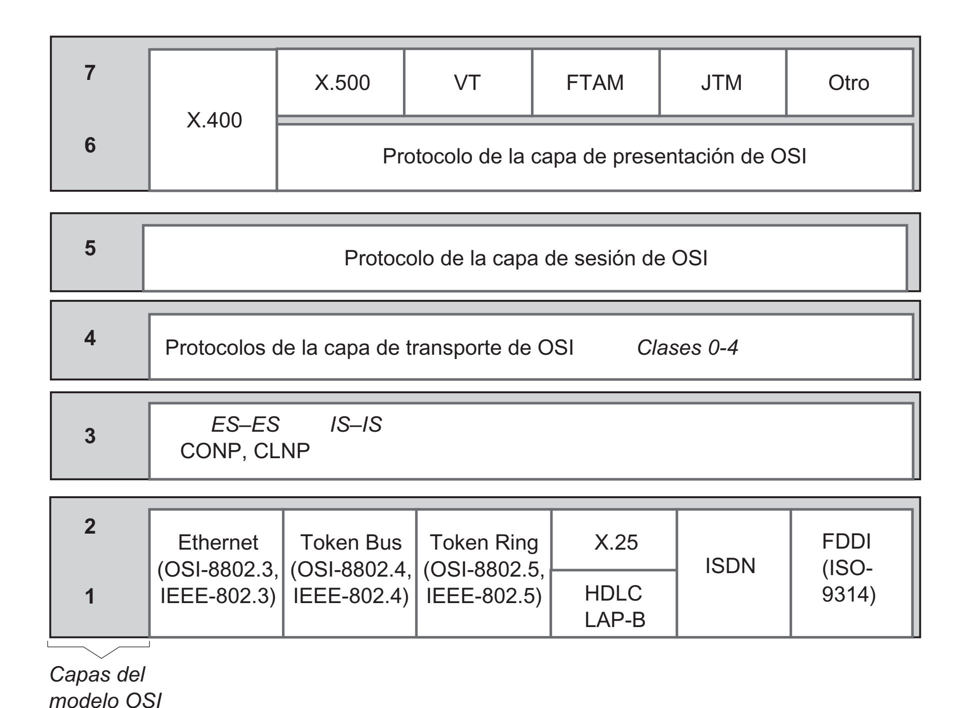


FIGURA 4.11 Pila de protocolos de OSI.

de enrutamiento siguientes: sistema intermedio-sistema terminal (ES-IS) y el sistema intermedio-sistema intermedio (IS-IS).

El protocolo de transporte de la pila OSI, de acuerdo con las funciones que tiene definidas siguiendo el modelo OSI, esconde las diferencias entre los servicios orientados a la conexión y los no orientados a la conexión, de tal forma que los usuarios reciban la calidad de servicio requerida independientemente de cuál sea la capa de red subyacente. Para asegurar lo anterior, la capa de transporte requiere que el usuario especifique la calidad de servicio que necesita.

La capa de aplicación incluye la transferencia de archivos, la emulación de terminal, los servicios de directorio y el correo electrónico. Los servicios más conocidos son el servicio de directorio (estándar X.500), el correo electrónico (X.400), el protocolo de terminal Virtual (VTP), el protocolo de transmisión, acceso y administración de archivos (FTAM) y el protocolo de la transferencia y administración de tareas (JTM).

Pila de protocolos IPX/SPX

La **pila de protocolos IPX/SPX** constituye la pila de protocolos original diseñada por Novell a principios de la década de 1980 en el sistema operativo de red, NetWare. La estructura de la pila de protocolos IPX/SPX y su correspondencia con el modelo OSI se muestra en la figura 4.12. Los protocolos de las capas de transporte y de red —intercambio de paquetes en las interredes (IPX) y el intercambio secuencial de paquetes (SPX)— dieron su nombre a toda la pila de protocolos. A la capa de red de esta pila de protocolos están también asociados los protocolos de enrutamiento: RIP y NLSP. Ejemplos representativos de las tres capas superiores son el protocolo de acceso remoto a los archivos NetWare: protocolo de núcleo NetWare (NCP) y el protocolo de publicidad del servicio (SAP).

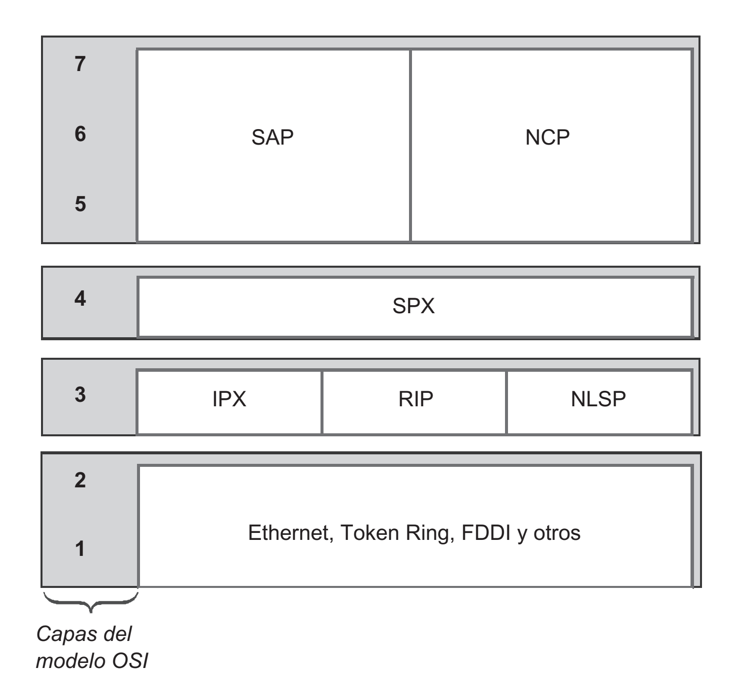


FIGURA 4.12 Pila de protocolos IPX/SPX.

NOTA *Hasta 1996, esta pila de protocolos era el líder mundial indiscutible en cuanto al número de instalaciones; sin embargo, la situación cambió de forma significativa y la pila de protocolos TCP/IP comenzó a ir a la delantera respecto a las otras pilas en cuanto a velocidad de crecimiento y número de instalaciones. Para 1998, TCP/IP se había convertido en el líder absoluto.*

Muchas características físicas de la pila de protocolos IPX/SPX pueden atribuirse a la orientación de las versiones anteriores de NetWare hacia las LAN pequeñas de PC, las cuales estaban caracterizadas por tener recursos limitados. Para lograr este objetivo, Novell requirió protocolos cuya implantación solamente necesitara una mínima cantidad de RAM (muy limitada en las PC compatibles con IBM que corrían con MS-DOS-640 KB solamente). Además, estos protocolos tenían que asegurar una operación rápida en dichas computadoras. Como resultado, los protocolos de la pila IPX/SPX, hasta fechas recientes, trabajaron muy bien en el ambiente de las LAN; sin embargo, en las grandes redes corporativas, saturaron en gran medida los lentos enlaces globales con los paquetes difundidos que son utilizados ampliamente por algunos protocolos de esta pila (por ejemplo, SAP). Además, la pila de protocolos IPX/SPX es propiedad de Novell y para implantarla tiene que comprarse una licencia, lo cual significa que no hay soporte para las especificaciones abiertas. Estas circunstancias han provocado que, por mucho tiempo, su uso se limite solamente a redes NetWare.

Pila de protocolos NetBIOS/SMB

La **pila de protocolos NetBIOS/SMB** fue diseñada por IBM y Microsoft (figura 4.13). En las capas física y de enlace de datos de esta pila de protocolos se utilizan la mayoría de los protocolos más populares, entre los que se incluyen Ethernet, *Token Ring* y FDDI. En las capas superiores de esta pila se usan los protocolos NetBEUI y smb.

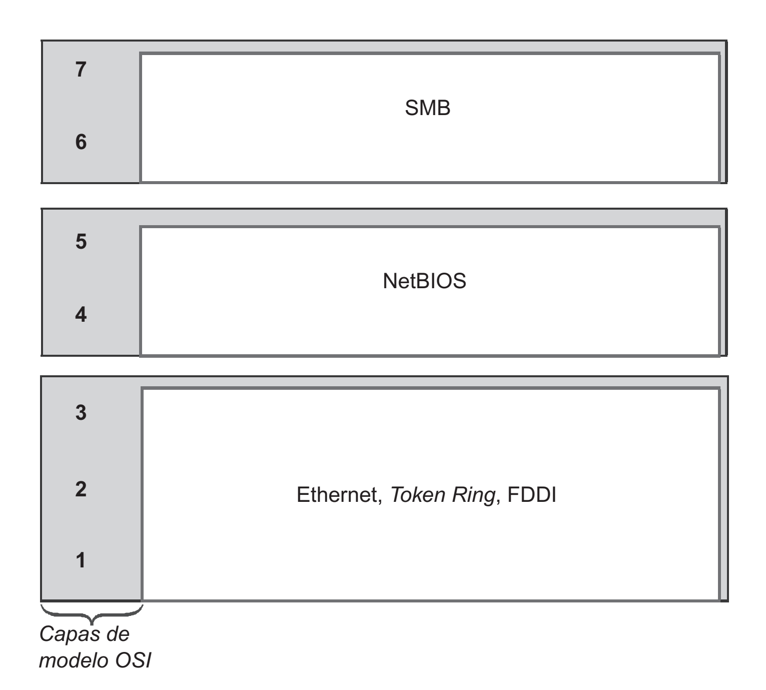


FIGURA 4.13 Pila de protocolos NetBIOS/SMB.

El protocolo del sistema básico de entrada/salida de la Red (NetBIOS, por sus siglas en inglés) apareció por primera vez en 1984 como una extensión de red de las funciones estándar BIOS de la PC de IBM para el software de Red de esa misma computadora. Después, este protocolo fue reemplazado por el protocolo de interfase de usuario extendido NetBIOS (NetBEUI). Para asegurar la compatibilidad de las aplicaciones, la interfase NetBIOS se mantuvo como una interfase del protocolo NetBEUI, diseñado como un protocolo eficaz con requerimientos bajos de recursos de cómputo hecho para redes pequeñas que tuvieran no más de 200 estaciones de trabajo. Este protocolo lleva a cabo un gran número de funciones de red de mucha utilidad que corresponden a las capas de transporte y de sesión del modelo OSI. Desafortunadamente, no permite el enrutamiento de paquetes, lo cual restringe el uso del protocolo NetBEUI a pequeñas LAN que no estén divididas en subredes e imposibilita su uso en interredes.

El protocolo de bloques de mensajes del servidor (SMB) lleva a cabo las funciones de las capas de sesión, presentación y aplicación del modelo OSI. Dicho protocolo sirve como base para implementar el servicio de archivos, así como para los servicios de impresión y mensajería.

Pila de protocolos TCP/IP

La **pila de protocolos TCP/IP** se diseñó como una iniciativa del Departamento de Defensa de Estados Unidos hace más de 20 años, con la finalidad de asegurar la conectividad entre la red experimental ARPANET y otras redes. La TCP/IP se implementó como un conjunto de protocolos para un ambiente de red heterogéneo. La Universidad de California en Berkeley aportó la mayor contribución al desarrollo de la pila de protocolos TCP/IP, nombrada de esta forma en honor a sus protocolos más importantes —IP y TCP—, al haber implementado los protocolos de esta pila en su versión del sistema operativo UNIX. La popularidad de

UNIX ha traído como resultado la prevalencia de TCP, IP y otros protocolos de dicha pila. En la actualidad, esta pila de protocolos se utiliza en las comunicaciones entre computadoras conectadas a Internet, así como en un gran número de redes corporativas.

Como la pila de protocolos TCP/IP fue originalmente desarrollada para Internet, tiene muchas ventajas sobre otros protocolos, en especial cuando se trata de construir redes que incluyan enlaces WAN. En particular, la capacidad de TCP/IP para fragmentar paquetes es de gran utilidad y permite usar esta pila de protocolos en redes de gran tamaño. Con frecuencia, una interred grande se construye a partir de varias redes que están basadas en principios muy diferentes. Para cada una de estas redes debe haber un valor específico en cuanto a la unidad máxima de transferencia (tamaño de trama). En este caso, cuando los datos se transfieren desde una red con una longitud de trama máxima más grande al de una red que tiene un valor más pequeño de este parámetro, es probable que sea necesario dividir la trama en varios segmentos. El protocolo de Internet de la pila de protocolos TCP/IP resuelve este problema de manera eficaz.

Otra de las ventajas de la tecnología TCP/IP es el sistema de direccionamiento flexible. Esta propiedad también promueve el uso del protocolo TCP/IP en el diseño de redes heterogéneas de gran tamaño.

La pila de protocolos TCP/IP utiliza sus características de difusión amplia de manera sencilla. Esta propiedad es absolutamente necesaria cuando se tienen enlaces lentos, los cuales todavía se usan a menudo en redes de larga distancia.

Sin embargo, como es costumbre, las ventajas tienen un precio; en este caso, las que se mencionaron previamente se obtienen a cambio de requerimientos más estrictos de los recursos y de la presencia de complicaciones en la administración de la red IP. Las capacidades funcionales poderosas de la pila de protocolos TCP/IP requieren una gran cantidad de recursos para su implementación. Un direccionamiento flexible y la falta de difusiones amplias (broadcast) hacen necesario tener varios servicios centralizados en las redes IP, como el sistema de nombre de dominio (DNS) y el DHCP. Cada uno de estos servicios tiene como objetivo facilitar los procedimientos de administración de la red; sin embargo, cada uno de ellos requiere mucha atención por parte de los administradores de red.

Se podrían mencionar otras ventajas y desventajas de la pila de protocolos TCP/IP; no obstante, esta pila de protocolos es la más conocida y la que en la actualidad se utiliza con mayor amplitud tanto en WAN como en LAN.

La arquitectura de la pila de protocolos TCP/IP se muestra en la figura 4.14. De manera similar que en el modelo OSI, TCP/IP tiene una estructura multicapa; sin embargo, TCP/IP se diseñó antes que el modelo ISO/OSI. La correspondencia de las capas de TCP/IP respecto a las del modelo OSI es muy condicional.

La pila de protocolos TCP/IP define cuatro capas:

La *capa de aplicación* de TCP/IP corresponde a las tres capas superiores del modelo OSI: las de aplicación, presentación y sesión; además, combina los servicios proporcionados por el sistema a las aplicaciones del usuario. Durante su operación en varias redes ubicadas en diferentes organizaciones y países, TCP/IP ha acumulado un gran número de protocolos y servicios de la capa de aplicación. La lista de dichos protocolos y servicios es muy larga e incluye protocolos ampliamente usados, como el protocolo de transferencia de archivos (FTP), el protocolo de emulación de terminal (telnet), el protocolo simple para la transferencia de correo (SMTP) y el protocolo de transferencia de hipertexto (http).

Los protocolos de la capa de aplicación están instalados en los **host**.[1]

[1] En la terminología de Internet, el nodo terminal tradicionalmente se llama **host** y el ruteador se denomina **Gateway (puerta de enlace)**. En este capítulo usaremos esta terminología.

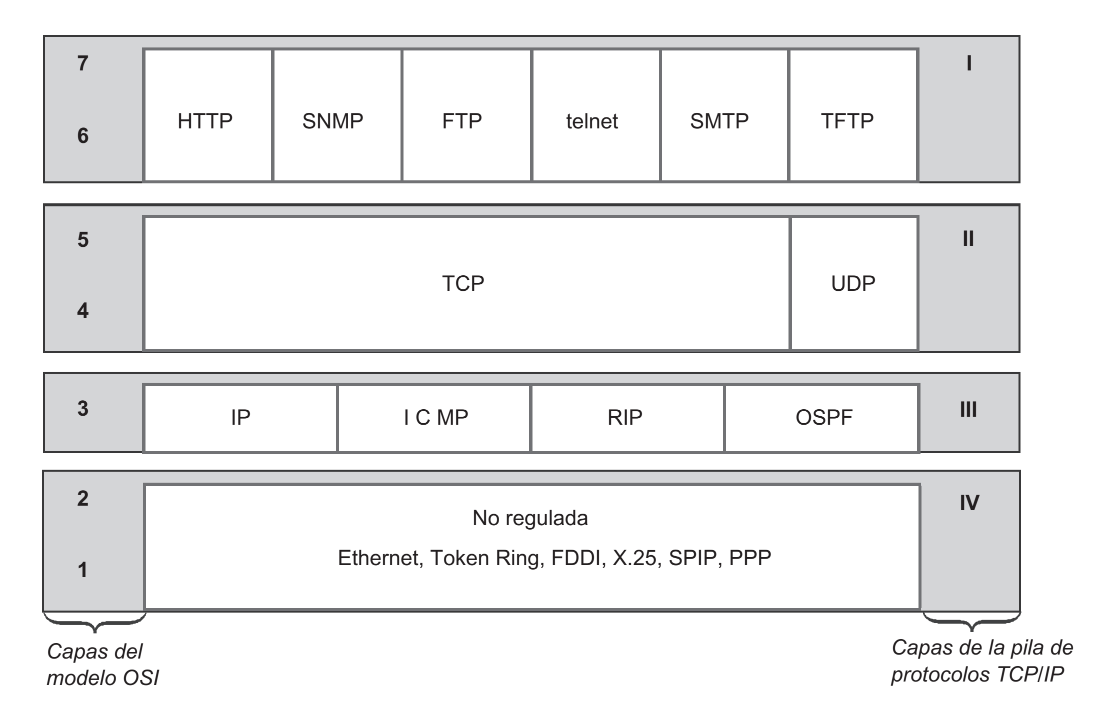


FIGURA 4.14 Arquitectura de la pila de protocolos TCP/IP.

La *capa de transporte* de la pila de protocolos TCP/IP puede proporcionar los dos tipos de servicios siguientes a la capa superior:

- Entrega garantizada: protocolo de control de la transmisión (TCP).
- Entrega con el mejor esfuerzo: protocolo de datagrama del usuario (UDP).

Para asegurar la entrega confiable de los datos, TCP toma sus previsiones con el fin de establecer una conexión lógica, la cual le permite numerar los paquetes, enviar un reconocimiento de su recepción y asegurar la retransmisión de cualquier paquete que se haya perdido. Asimismo, puede detectar y eliminar paquetes duplicados y entregar los paquetes a la capa de aplicación en el orden en que fueron enviados. Este protocolo facilita que los objetos en las computadoras de origen y destino puedan soportar el intercambio de datos en modo dúplex. El protocolo TCP asegura la entrega libre de errores del flujo de bytes que se forma en una computadora y va a cualquier otra computadora conectada a la interred. La TCP divide el flujo de bytes en fragmentos y los envía a la capa inferior, a la interred. Después de que dichos fragmentos son entregados —con ayuda de las herramientas de la conectividad de redes— a la computadora de destino, TCP los reensambla para formar un flujo continuo de bytes.

El segundo protocolo de esta capa —UDP— es el protocolo de datagrama más simple que se utiliza cuando el problema del intercambio confiable de datos no se presenta o está resuelto mediante las herramientas de una capa superior, la capa de aplicación o las aplicaciones del usuario.

Las funciones de los protocolos TCP y UDP incluyen el papel que desempeña el enlace entre la capa de aplicación y la capa inferior de la interred. La capa de transporte lleva a cabo la tarea de transmitir datos con la calidad especificada desde la capa de aplicación y le informa después de que ha terminado la tarea. Por otro lado, TCP y UDP utilizan la capa inferior de la interred como un tipo de herramienta, la cual no se caracteriza por tener una

alta confiabilidad; sin embargo, puede transmitir el paquete a través de la interred. De manera similar a los protocolos de la capa de aplicación, TCP y UDP se instalan en host.

La *capa de red*, también llamada *capa interred*, se encuentra en el núcleo de la arquitectura TCP/IP. Las funciones de esta capa corresponden a las de la capa de red del modelo OSI y aseguran la transferencia de paquetes dentro de la interred, la cual se crea mediante la conexión de varias redes. Los protocolos de la capa de red soportan la interfase hacia la capa de transporte que está más arriba y reciben de ésta las solicitudes para la transmisión de datos utilizando la interred y de ahí hacia la capa de interfase de red, cuyas funciones serán estudiadas más adelante.

El protocolo Internet (IP) es el más importante de la capa de interred. Entre sus funciones se encuentra el envío de paquetes entre redes —de un ruteador a otro— hasta que el paquete llega a la red a la que está destinado. En contraste con los protocolos de las capas de aplicación y de transporte, IP está instalado no sólo en todos los host sino también en todas las puertas de enlace (Gateway). El IP es un protocolo de datagrama no orientado a la conexión que trabaja de acuerdo con el principio del mejor esfuerzo.

Los protocolos que realizan funciones auxiliares en relación con IP a menudo se clasifican como pertenecientes a la capa de red de TCP/IP. En la lista de estos protocolos se incluyen el protocolo de información de enrutamiento (RIP) y la primera trayectoria abierta más corta (OSPF), que tienen que ver con el estudio de la topología de la red, la determinación de las rutas y la creación de tablas de enrutamiento que ayudan en el envío de paquetes en la dirección que se necesita. Por la misma razón, existen otros dos protocolos que también pueden clasificarse como pertenecientes a la capa de red: el protocolo de mensajes de control de Internet (ICMP) —diseñado para transmitir información acerca de los errores en la transmisión de paquetes del ruteador a la fuente de la información— y el protocolo de administración del grupo de Internet (IGMP), utilizado para el envío de paquetes a varias direcciones de forma simultánea.

Las diferencias ideológicas de la arquitectura de la pila de protocolos TCP/IP respecto a la organización multicapa de otras pilas de protocolos radica en la interpretación de las funciones de las capas inferiores. Éstas son las funciones de la *capa de interfase de red.*

Recuerde que las capas inferiores del modelo OSI (las capas de enlace de datos y física) llevan a cabo muchas de las funciones responsables del acceso al medio de transmisión: el tramado, la coordinación de los niveles de las señales eléctricas, la codificación, la sincronización, etc. Todas estas funciones específicas constituyen la esencia de los protocolos de intercambio de datos, como Ethernet, *Token Ring*, PPP, HDLC y muchos otros.

La capa inferior de la pila de protocolos de TCP/IP resuelve un problema significativamente más sencillo: es responsable solamente de organizar la interacción con las tecnologías de red utilizadas en las redes que forman la interred. La TCP/IP considera cualquier red incluida en la interred como una herramienta para el transporte de paquetes al ruteador siguiente dentro de la ruta.

De lo anterior se infiere que la tarea de proporcionar una interfase entre la tecnología TCP/IP y cualquier otra tecnología de la red intermedia se reduce a las siguientes tareas:

- La definición del método de encapsulamiento de paquetes IP en la PDU de la red intermedia.
- La determinación del método para traducir las direcciones de red en direcciones correspondientes a la tecnología utilizada por este nodo intermedio.

Dicho método hace que la interred TCP/IP esté abierta para la incorporación de cualquier otra red, independientemente de la tecnología de transmisión de datos interna que esa red utilice. Por cada tecnología empleada en una red que sea parte de la interred, es necesario desarrollar herramientas de interfase específicas. De aquí que las funciones de esta capa no pueden definirse de manera permanente.

La capa de interfase de red de la pila de protocolos TCP/IP no está regulada estrictamente, es decir, soporta todas las tecnologías de red más comunes. Para las LAN, éstas son Ethernet, *Token Ring*, FDDI, Fast Ethernet y Ethernet Gigabit; para las WAN, éstas son protocolos punto a punto como el SLIP y el PPP; para las redes de conmutación de circuitos, éstas son las tecnologías X.25, *Frame Relay* y ATM.

En general, cuando surge una nueva tecnología de LAN o WAN se incluye a la brevedad en la pila de protocolos TCP/IP mediante el desarrollo del RFC apropiado, el cual determina el método de encapsulamiento de los paquetes IP en sus tramas. Por ejemplo, el RFC 1577, el cual define el funcionamiento de IP en las redes ATM, apareció en 1994, poco después de que se adoptaron los estándares principales de ATM.

NOTA *Observe que la pila de protocolos TCP/IP permite la inclusión de redes componentes en la interred sin importar el número de capas en esas redes. Así, la transmisión de datos en las redes X.25 es asegurada por los protocolos de las capas física, de enlace de datos y de red (de acuerdo con la terminología de OSI); sin embargo, la pila de protocolos TCP/IP considera a la red X.25 y a otras tecnologías solamente como herramientas para el transporte de paquetes IP entre dos puertas de enlace fronterizas. La capa de interfase de red proporciona a esta tecnología el método de encapsulamiento de paquetes IP en un paquete X.25, así como las técnicas de traducción de direcciones IP en direcciones de la capa de red de X.25. Si esta organización de red concuerda estrictamente con el modelo OSI, será necesario admitir la presencia de una contradicción explícita: un protocolo de la capa de red (IP) trabaja sobre otro protocolo de la capa de red (X.25). No obstante, esto es muy normal en el caso de TCP/IP.*

Cada protocolo de comunicaciones manipula una unidad específica de datos transmitidos. Los nombres de las convenciones de estas unidades se especifican a menudo en el estándar y con mucha frecuencia se definen por tradición. Durante la larga existencia de la pila de protocolos TCP/IP se ha adoptado terminología específica (figura 4.15).

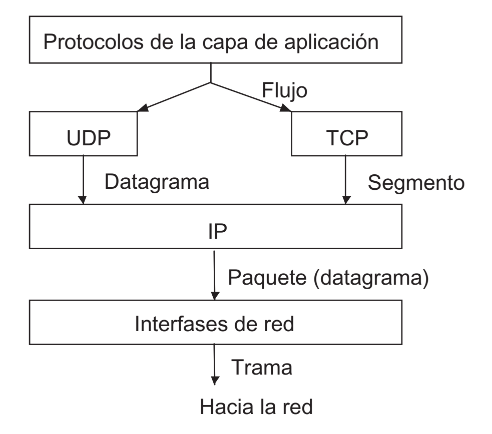


FIGURA 4.15 Nombres de PDU del TCP/IP.

Flujo es el término que se emplea para designar el arribo de datos desde las aplicaciones hasta la entrada de los protocolos de la capa de transporte, TCP y UDP.

TCP divide el flujo en **segmentos**.

La unidad de datos del protocolo del UDP a menudo se conoce como **datagrama**, el cual es el nombre común de los PDU que utilizan los protocolos no orientados a la conexión. En la lista de dichos protocolos se incluye el protocolo IP; por lo tanto, su PDU se llama también datagrama. Sin embargo, con frecuencia se usa otro término: paquete IP.

De acuerdo con la terminología de TCP/IP, las **tramas** son PDU de cualquier tecnología en las que los paquetes IP se encapsulan para su subsecuente transporte a través de las redes que constituyen la interred. En este caso, no importa qué nombre se utilice para este PDU en la tecnología de una red específica. Por ende, la trama de Ethernet, la celda ATM y el paquete X.25 son considerados tramas por la pila de protocolos TCP/IP, ya que todos estos PDU se interpretan como contenedores dentro de los cuales viaja un paquete IP a través de Internet.

4.4.5 Correspondencia entre pilas de protocolos populares y el modelo OSI

La figura 4.16 muestra la correspondencia entre las pilas de protocolos estándares y el modelo de referencia OSI. Como puede observar, esta correspondencia es muy convencional. En la mayoría de los casos, los diseñadores sacrifican la estructura modular a cambio de mayor velocidad de operación. Solamente la pila de protocolos OSI se divide en siete capas. Muy a menudo, las pilas de protocolos se dividen en tres o cuatro capas: la capa de adaptación de red (donde se hallan implementadas las capas física y de enlace de datos del modelo OSI), la capa de red, la capa de transporte y la capa de servicios, la cual combina las funciones de las capas de sesión, presentación y aplicación del modelo OSI.

Modelo OSI	IBM/Microsoft	TCP/IP	Novell	Pila de protocolos OSI
Aplicación	SMB	Telnet, FTP, SNMP, SMTP, WWW	NCP, SAP	X.400 X.500 FTAM
Presentación				OSI presentación
Sesión	NetBIOS	TCP		OSI sesión
Transporte			SPX	OSI transporte
Red		IP, RIP, OSPF	IPX, RIP NLSP	ES-ES IS-IS
Enlace de datos	802.3 (Ethernet), 802.5 (Token Ring), Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP			
Física	Cable coaxial, par trenzado con y sin protección, fibra óptica y ondas de radio			

FIGURA 4.16 Correspondencia entre pilas de protocolos conocidos y las capas del modelo OSI.

Además de lo anterior, existen otras razones por las que la estructura de las pilas de protocolos a menudo no está de acuerdo con las recomendaciones de OSI. Recuerde las características ideales de la descomposición multicapa. Primero, es necesario observar el principio de la jerarquía: cada una de las capas superiores solicita solamente a su capa inferior más cercana y las capas inferiores proporcionan servicios sólo a la capa superior más cercana. En las pilas de protocolos, esto da como resultado que el PDU de la capa superior siempre se encapsule en el PDU de la capa inferior.

Segundo, la descomposición ideal multicapa asume que todos los módulos de la misma capa son responsables de llevar a cabo la tarea; sin embargo, a menudo estos requerimientos contradicen la construcción real de las pilas de protocolos. Por ejemplo, la función principal de la capa de red de TCP/IP (parecida a la capa de red de la pila de protocolos OSI) es asegurar la transmisión de paquetes usando la interred. La pila de protocolos TCP/IP ofrece varios protocolos para resolver este problema. Como ejemplos se tiene el IP, que se utiliza para el envío de paquetes, así como el RIP y el OSPF, los cuales son protocolos de enrutamiento. Si los protocolos que resuelven la tarea se consideran un signo de que dichos protocolos pertenecen a la misma capa, los protocolos de Internet y de enrutamiento deben pertenecer a la misma capa. Sin embargo, los mensajes RIP están encapsulados en datagramas UDP y los OSPF se encapsulan en paquetes IP; por lo tanto, si se sigue formalmente la estructura jerárquica de la pila, el protocolo OSPF debe pertenecer a la capa de transporte y el RIP debe pertenecer a la capa de aplicación. No obstante, en la práctica, los protocolos de enrutamiento se consideran generalmente protocolos de la capa de red.

4.5 SERVICIOS DE INFORMACIÓN Y TRANSPORTE

PALABRAS CLAVE: servicios de transporte, servicios de información, redes de infocomunicación, RIP, OSPF, BGP, traducción de direcciones, administración de la red, plano del usuario, plano de control, plano de administración y protocolo simple de la administración de la red (SNMP).

Los servicios de una red de computadoras pueden clasificarse en las dos categorías siguientes:

- Servicios de transporte
- Servicios de información

Los **servicios de transporte** suponen que los datos se transmiten entre los diferentes usuarios de la red sin que éstos sean modificados. La red ingresa los datos de un usuario en una de sus interfases, los transmite a través de los switches de tránsito y envía los datos a otro usuario mediante otra interfase. Cuando se proporcionan los servicios de transporte, la red no cambia la información que se transmite. En lugar de eso, lleva los datos al receptor de la misma forma como el emisor los proporcionó a la red. Un ejemplo de un servicio de transporte proporcionado por las WAN es la interconexión de una LAN del cliente.

Los **servicios de información** consisten en ofrecer al usuario información novedosa. Estos siempre están relacionados con las operaciones de procesamiento de datos: almacenamiento en forma ordenada (sistema de archivos o base de datos), búsqueda de la información que se requiera y su presentación en la forma que se necesite. Los servicios de información existían mucho antes del arribo de las primeras redes de computadoras. El servicio de consultas de directorio que proporcionan las redes telefónicas es un ejemplo típico de un servicio de información. Con la llegada de las computadoras, los servicios de información han expe-

rimentado una revolución, debido a que la computadora se inventó para el procesamiento automático de información. Para proporcionar servicios de información se utilizan varias tecnologías de la información: como la programación, las bases de datos, los archivos, el WWW y el correo electrónico.

En las redes de telecomunicaciones que existían antes de la llegada de la computadora, los servicios de transporte siempre prevalecieron. La transmisión de tráfico de voz entre suscriptores siempre fue el servicio principal de las redes telefónicas, mientras que los servicios por demanda eran complementarios. En las redes de computadoras, ambos tipos de servicios son igualmente importantes. Esta característica se refleja en el nombre de la nueva generación de redes de telecomunicaciones que ha surgido como resultado de la convergencia de varios tipos de redes. En la actualidad, dichas redes a menudo se llaman **redes de infocomunicación**. Este nombre todavía no es aceptado comúnmente, aunque refleja muy bien las nuevas tendencias, incluidos ambos componentes de los servicios de red en los mismos términos.

La clasificación de los servicios de las redes de computadoras en dos categorías se manifiesta de muchas formas. Por ejemplo, en la actualidad existe una división estricta entre los especialistas en el campo de las redes de computadoras. Por un lado, están los profesionales en tecnologías de la información y por otro los profesionales en redes. La primera categoría de especialistas incluye programadores, diseñadores de bases de datos, administradores de sistemas operativos y diseñadores web, esto es, todos los especialistas involucrados en el desarrollo y soporte de software y hardware de computadoras. La segunda categoría incluye especialistas involucrados en la solución de problemas de transporte en redes, que tienen que ver con enlaces y equipo de comunicaciones tales como switches, ruteadores y concentradores. Resuelven los problemas relacionados con la selección de la topología de las redes, la definición de las rutas de los flujos de tráfico, la definición del ancho de banda requerido para los enlaces y el equipo de comunicaciones, así como otros asuntos relacionados exclusivamente con la transmisión de tráfico a través de las redes.

Es indudable que cada categoría de especialistas debe conocer los problemas y métodos de las áreas relacionadas. Los que están involucrados en el desarrollo de las aplicaciones distribuidas deben comprender qué servicios de transporte pueden obtener a partir de la red, con el fin de organizar una operación coordinada de los componentes distribuidos de sus aplicaciones. Por ejemplo, los programadores de redes deben saber que la pila de protocolos TCP/IP proporciona dos tipos de transporte diferentes: TCP y UDP. Por lo tanto, depende del programador la decisión acerca de cuál de estos servicios se adecua más a la aplicación específica. De manera similar, un diseñador de herramientas de transporte de red debe saber cuáles son los requerimientos de la aplicación para la transmisión de tráfico, a fin de tenerlos en cuenta en el diseño de la red. Aun así, la especialización en las áreas de IT y de redes existe, lo cual refleja el doble propósito de las redes de computadoras.

La clasificación de los servicios de red en transporte e información también se refleja en la organización de las pilas de protocolos, así como en la distribución de los componentes de las diversas pilas de protocolos en elementos de red.

4.5.1 Distribución de protocolos por elementos de la red

La figura 4.17 muestra los componentes principales de las redes de computadoras: nodos terminales o computadoras y nodos de paso o switches y ruteadores. Para este ejemplo se seleccionaron los protocolos de la pila TCP/IP, ya que son los más comunes.

A partir de la figura, es evidente que la pila de protocolos completa está implementada sólo en los nodos terminales; los nodos de paso soportan los protocolos de las tres capas infe-

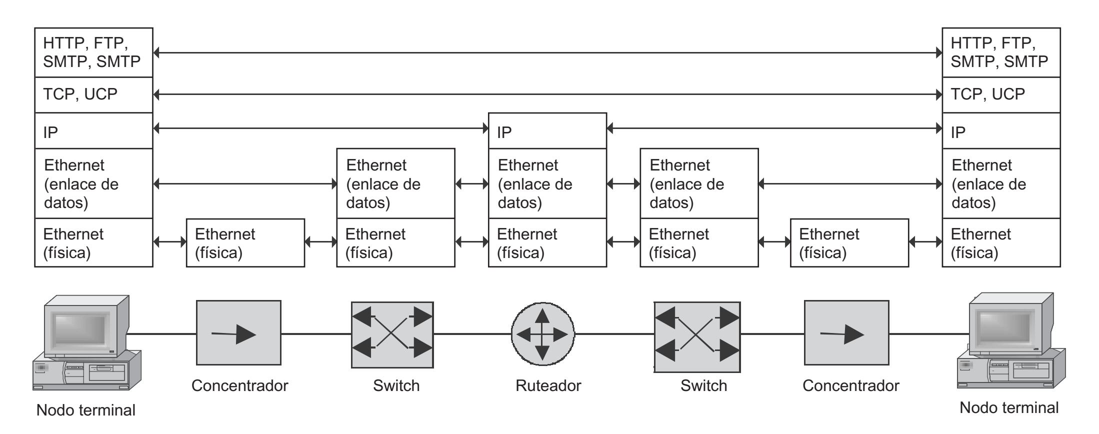


FIGURA 4.17 Correspondencia entre las funciones de los dispositivos de la red y las capas del modelo OSI.

riores. Esto puede explicarse mediante las capacidades funcionales de las tres capas inferiores, ya que éstas son suficientes para los dispositivos de comunicaciones que envían paquetes; además, un dispositivo de comunicaciones únicamente puede soportar los protocolos de las dos capas inferiores o, a veces, sólo los de la capa física: esto depende del tipo de dispositivo de que se trate.

- *Concentrador*: trabaja con los flujos de bits y, por lo tanto, su operación está limitada al soporte del protocolo de la capa física.
- *Switches LAN*: soportan los protocolos de las dos capas inferiores (la física y la de enlace de datos) y de esta forma les permite operar dentro de los límites de las topologías estándar.
- *Ruteadores*: deben soportar protocolos de las tres capas inferiores, puesto que necesitan a la capa de red para interconectar redes con base en diferentes tecnologías. Son necesarios los protocolos de las dos capas inferiores para interactuar con las redes componentes (por ejemplo, Ethernet o *Frame Relay*).
- *Interruptores o switches WAN*: los interruptores de las WAN como ATM, que operan con base en circuitos virtuales, pueden soportar dos o tres capas de protocolos. El protocolo de la capa de red se requiere cuando los switches soportan los procedimientos para establecer circuitos virtuales de modo automático. Puesto que la topología de una WAN es arbitraria, no se puede prescindir de un protocolo de red. Por otro lado, si los administradores de red configuran los circuitos virtuales en forma manual, será suficiente con que el switch WAN soporte solamente los protocolos de las capas física y de enlace de datos para la transmisión de datos a través de circuitos virtuales existentes.

Las computadoras que corren aplicaciones de red deben soportar protocolos de todas las capas. Los protocolos de la capa de aplicación, mediante el uso de servicios proporcionados por los protocolos de las capas de sesión y presentación, brindan a las aplicaciones un conjunto de servicios de red en forma de un API de red. El protocolo de la capa de transporte también opera en todos los nodos terminales. Cuando es necesario organizar la transmisión de datos utilizando la red, interactúan dos entidades del protocolo de transporte que operan en los nodos de transmisión y recepción con el fin de asegurar que se proporcione la calidad requerida del servicio de transporte. Los dispositivos de comunicaciones de la red entregan

los mensajes del protocolo de transporte de una manera transparente, sin tener nada que ver con el contenido de dichos mensajes.

En las computadoras, los protocolos de comunicaciones de todas las capas (excepto la capa física y algunas funciones de la capa de enlace de datos) se implementan mediante software del sistema.

Los nodos terminales de la red (computadoras y dispositivos de alta tecnología basados en computadoras, como los teléfonos móviles) siempre brindan servicios de información y transporte, mientras que los nodos de la red de tránsito únicamente proporcionan servicios de transporte. Si una red ofrece sólo servicios de transporte, esto significa que los nodos terminales están fuera de la frontera de la red. En general, éste es el caso de las redes comerciales que ofrecen servicios a sus clientes. Si decimos que una red también proporciona servicios de información, esto significa que las computadoras que brindan estos servicios son parte de la red. Un ejemplo típico de esta situación es aquella en la que un proveedor del servicio de Internet, además de ofrecer al acceso a esta red, también da soporte a sus propios servidores web.

4.5.2 Protocolos subsidiarios del sistema de transporte

Como es evidente, la figura 4.17 mostró una versión simplificada de la distribución de protocolos en los diferentes elementos de la red. En las redes prácticas, ciertos dispositivos de comunicaciones no sólo soportan protocolos de las tres capas inferiores, sino también de las capas superiores. Por ejemplo, los ruteadores implementan protocolos de enrutamiento con el propósito de construir tablas de enrutamiento de manera automática. A menudo, los concentradores y los switches soportan los protocolos SNMP y telnet, los cuales no son estrictamente necesarios para llevar a cabo las funciones principales de estos dispositivos; sin embargo, estos protocolos permiten configurarlos y controlarlos de forma remota. Todos estos protocolos son de la capa de aplicación y llevan a cabo algunas funciones auxiliares del sistema de transporte. Obviamente, con la finalidad de soportar protocolos de la capa de aplicación, el equipo de la red también debe soportar protocolos de la capa intermedia, como el IP y el TCP/UDP.

Los protocolos subsidiarios pueden dividirse en grupos de acuerdo con sus funciones.

El primer grupo incluye *protocolos de enrutamiento,* como el RIP, OSPF y BGP. Sin estos protocolos, los ruteadores no podrían enrutar paquetes, ya que la tabla de enrutamiento permanecería vacía (a menos que el administrador de la red la llenara de modo manual, lo que no es una solución apropiada en redes de gran tamaño). Si consideramos no sólo la pila de protocolos TCP/IP, sino también las pilas de protocolos de las redes que soportan circuitos virtuales, este grupo incluiría los protocolos utilizados para la configuración de circuitos virtuales.

Otro grupo de protocolos subsidiarios se encarga de la **traducción de direcciones**. En particular, se incluye el protocolo DNS, el cual traduce nombres de nodos simbólicos en direcciones IP. Otro protocolo de este grupo, el DHCP, permite que las direcciones IP se asignen en forma dinámica a los host de la red. Esto contrasta con las direcciones IP estáticas, las cuales los administradores de la red deben asignar en forma manual. Por lo tanto, las tareas de los administradores de la red se simplifican.

En el tercer grupo se incluyen protocolos que se utilizan para la **administración de la red.** Con este propósito, la pila de protocolos TCP/IP incluye el protocolo simple para la administración de redes (SNMP), el cual permite la colección, de modo automático, de información acerca de los errores y fallas en los dispositivos, así como el protocolo telnet, que utilizan los administradores de redes para configurar switches y ruteadores de manera remota.

Cuando se consideran los protocolos subsidiarios hemos encontrado situaciones en las que la clasificación jerárquica de los protocolos mediante capas (es decir, división vertical) adoptada en el modelo OSI demuestra ser insuficiente. Además de las capas jerárquicas, también es necesario dividir la clasificación horizontal de protocolos en varios grupos.

A pesar de que el modelo OSI no cuenta con dicha división, en la práctica sí existe. De hecho, este método se utilizó en la estandarización de las redes ISDN, el cual, como se mencionó, utiliza tanto la técnica de conmutación de circuitos como la de paquetes. Los estándares de ISDN clasifican todos los protocolos en tres grupos, llamados plano del usuario, plano de control y plano de administración (figura 4.18).

- El grupo **plano del usuario** incluye los protocolos necesarios para transmitir el tráfico de voz del usuario.
- El grupo **plano de control** incluye los protocolos que se requieren para establecer las conexiones de la red.
- El grupo **plano de administración** conecta a los protocolos que soportan las operaciones de administración de la red, como la detección de errores y el análisis de la configuración de dispositivos.

A partir de esta descripción, resulta claro que existen analogías directas entre las funciones de los planos y los grupos de funciones subsidiarias de las redes de computadoras basadas en TCP/IP y otras tecnologías. Aunque dicha división horizontal de protocolos no es ampliamente aceptada en las redes de computadoras, aún es de utilidad, ya que ayuda a comprender mejor el propósito de cada protocolo. Además, la clasificación horizontal ayuda a explicar los problemas de correlacionar algunas de las capas del modelo OSI. Por ejemplo, algunos autores ubican a los protocolos de enrutamiento en la capa de red, mientras que otros los clasifican como parte de la capa de aplicación. Esto no se debe a negligencia de los autores, sino que es provocado por las dificultades objetivas de la clasificación. El modelo OSI es muy apropiado para estandarizar los protocolos involucrados en el transporte del tráfico del usuario (es decir, los protocolos que pueden clasificarse como pertenecientes al plano del usuario). Sin embargo, es significativamente poco apropiado para la estandarización de protocolos subsidiarios. Por lo tanto, muchos autores ubican los protocolos de

Plano del usuario	Plano de control	Plano administrativo
Capa de aplicación	Capa de aplicación	Capa de aplicación
Capa de presentación	Capa de presentación	Capa de presentación
Capa de sesión	Capa de sesión	Capa de sesión
Capa de transporte		
Capa de red		
Capa de enlace de datos		
Capa física		

FIGURA 4.18 Tres grupos de protocolos.

enrutamiento en la capa de red, con el fin de reflejar su parecido funcional a los servicios de transporte de la red implantada por IP.

RESUMEN

- El modelo eficaz de interacción de redes entre computadoras es la estructura multicapa, en la que los módulos de las capas superiores utilizan las herramientas de la capa inferior como instrumentos para llevar a cabo sus tareas. Cada capa soporta dos tipos de interfases: las interfases de servicio con las capas superiores e inferiores de la jerarquía de herramientas de red del nodo, y la interfase de igual a igual con las herramientas de la misma capa que corre en el nodo remoto. Esta última interfase se conoce como *protocolo*.
- Una pila de protocolos es un conjunto de protocolos para la interacción jerárquica entre los nodos de una red. Los protocolos de las capas inferiores a menudo están implementados mediante combinaciones de software y hardware. Los protocolos de las capas superiores por lo general se implementan con base en herramientas de software. Los módulos de software que establecen un protocolo específico se llaman *entidades del protocolo*.
- A principios de la década de 1980, el ISO, la ITU-T y otras organizaciones internacionales que trabajan en el campo de la estandarización desarrollaron el modelo OSI estándar. Dicho modelo contiene descripciones de la representación generalizada de herramientas para la conectividad de redes. Se utiliza como un tipo de idioma universal para los profesionales en redes; por lo tanto, se conoce como modelo de referencia. El modelo OSI define siete capas de interacción, les asigna nombres estándar y especifica las funciones que debe realizar cada capa.
- *Un sistema abierto es cualquier sistema* (computadora, red de computadoras, producto de software, sistema operativo o cualquier otro software o hardware) construido de acuerdo con especificaciones del dominio público, correspondiente a estándares y adoptado por las partes interesadas, como resultado de un análisis público.
- Según del estatus de las organizaciones, es posible clasificar sus estándares de acuerdo con las categorías siguientes: estándares propietarios de compañías específicas, estándares diseñados por comités especializados, estándares nacionales y estándares internacionales.
- El avance más significativo en cuanto a estandarización en el campo de las redes de computadoras lo constituye la estandarización de los protocolos de comunicaciones. En la lista de las pilas de protocolos estandarizados se incluyen TCP/IP, IPX/SPX, NetBIOS/SMB, OSI, DECnet y SNA. La posición líder pertenece a la pila de protocolos TCP/IP, la cual se utiliza para las comunicaciones entre decenas de millones de computadoras que participan en la red mundial de la información: Internet. La pila de protocolos TCP/IP tiene cuatro capas: de aplicación, de transporte, de interred e interfases de red. La correspondencia entre las capas de TCP/IP y las de OSI es convencional.

PREGUNTAS DE REPASO

1. ¿Qué estandariza el modelo OSI?
2. ¿Es posible presentar otra variante de OSI que contenga un número de capas diferente, por ejemplo: cinco u ocho?

3. ¿Es el protocolo el módulo de software que resuelve el problema de la interacción entre sistemas, o éste representa una descripción formal de las reglas de interacción, incluida la secuencia del intercambio de mensajes y sus formatos?
4. ¿Son sinónimos los términos *interfase* y *protocolo*?
5. ¿En qué capa del modelo OSI operan los programas de aplicación?
6. ¿Sobre qué elementos de la red se encuentran instalados los protocolos de la capa de transporte?
7. ¿En qué capa del modelo OSI trabajan los servicios de red?
8. ¿Cuáles dispositivos de los que se relacionan a continuación llevan a cabo las funciones de la capa física del modelo OSI? y ¿cuáles son los que implementan la capa de enlace de datos?
   a) Ruteador
   b) Switch
   c) Puente
   d) Repetidor
   e) Adaptador de red
9. ¿Qué nombres se han utilizado tradicionalmente para la unidad de datos del protocolo en cada capa? Complete la tabla.

	Paquete	Mensaje	Trama	Flujo	Segmento
Capa de enlace de datos					
Capa de red					
Capa de transporte					
Capa de sesión					
Capa de presentación					
Capa de aplicación					

10. Proporcione ejemplos de sistemas abiertos.
11. Suponga que una pequeña compañía, no muy conocida, ofrece un producto que usted necesita, caracterizado por parámetros que exceden a los de productos similares vendidos por compañías bien establecidas. Usted podría aceptar la oferta después de revisar la documentación del fabricante y asegurarse de que en realidad especifica los parámetros que exceden los parámetros equivalentes de productos bien conocidos. O usted podría aceptar la oferta solamente después de hacer una minuciosa prueba que confirmara que los parámetros técnicos del producto en consideración son mejores que los de productos similares disponibles en el mercado. O bien podría seleccionar el producto de una compañía muy establecida, puesto que está garantizado que cumple con los estándares y no existe ningún riesgo de que quede fuera del mercado y, en consecuencia, no habrá problemas cuando se necesite soporte técnico. ¿En qué caso su acción cumplirá con el principio de los sistemas abiertos?
12. ¿Qué organización diseñó los estándares de Ethernet?
13. ¿Cuál de las fuerzas administrativas de Internet está directamente involucrada con la estandarización?
14. ¿Son sinónimos los términos *estándar*, *especificación* y *RFC*?

15. ¿Qué tipo de estándares representan los RFC actuales?
    a) Estándares propietarios
    b) Estándares gubernamentales
    c) Estándares nacionales
    d) Estándares internacionales
16. ¿Qué organización dio pie a la creación y estandarización de la pila de protocolos TCP/IP?
17. Especifique las propiedades principales de la pila de protocolos TCP/IP.
18. Compare las funciones de las capas inferiores de los modelos de referencia TCP/IP y OSI.
19. Defina los servicios de transporte e información.
20. ¿Qué protocolos pertenecen al plano de control?, ¿cuáles pertenecen al plano de administración?
21. ¿Es necesario que los ruteadores soporten los protocolos de la capa de transporte?

PROBLEMAS

1. Suponga que usted tiene dos computadoras conectadas a una red que utiliza adaptadores Ethernet. Los controladores del adaptador que están instalados en dichas computadoras soportan diferentes interfases hacia la capa de red del protocolo IP. ¿Interactuarán las computadoras de manera normal?
2. Cómo podría usted organizar la interacción entre dos computadoras, si éstas utilizan protocolos distintos en las capas siguientes:
    - ¿Física y de enlace de datos?
    - ¿De red?
    - ¿De aplicación?
3. Describa los pasos que usted debería seguir si tuviera que verificar el estado del proceso de estandarización de la tecnología MPLS.
4. Investigue el área en la que el IETF ha concentrado sus esfuerzos (por ejemplo, a través del número de grupos de trabajo).

5

EJEMPLOS DE REDES

DESCRIPCIÓN DEL CAPÍTULO

5.1 INTRODUCCIÓN

En este capítulo se describe la arquitectura organizacional de los tipos de redes más conocidos: redes de telecomunicaciones de larga distancia, redes corporativas e Internet.

A pesar de las diferencias entre tales tipos de redes, éstas tienen mucho en común. Primero, sus arquitecturas son similares; por ejemplo, cualquier red de telecomunicaciones consiste en una troncal (backbone), redes de acceso, centros de información y equipo del cliente. Como es natural, este diseño generalizado tiene un contenido específico de información para cada tipo de red.

Las redes de telecomunicaciones de larga distancia son diferentes en el sentido que proporcionan un servicio público. Tradicionalmente, en la lista de servicios que brindan se encuentran algunos de telefonía y otros de líneas arrendadas a organizaciones que construyen sus propias redes. A medida que las redes de computadoras se han difundido, las compañías de larga distancia han incrementado de forma significativa el rango de sus servicios. Por ejemplo, en la actualidad, la mayoría proporciona acceso a Internet, redes privadas virtuales (VPN), hospedaje web, correo electrónico, telefonía IP, audio y difusión de video.

A mediados de la década de 1980, la eliminación de monopolios en esta área comenzó en todo el mundo. Como consecuencia, a las compañías de telecomunicaciones de larga distancia se les prohibió proporcionar servicios públicos, lo que tuvo como consecuencia el arribo de compañías proveedoras de larga distancia competitivas, las cuales trataron de atraer clientes mediante el ofrecimiento de un portafolios de servicios más extenso y una relación costo-beneficio más atractiva en sus servicios. Conocer la estructura administrativa del mundo de las telecomunicaciones es útil para comprender las características específicas de las tecnologías de las redes, las cuales, en algunos casos, están diseñadas especialmente para compañías de larga distancia de un tipo determinado.

Las redes corporativas tienen una estructura jerárquica similar a la de las compañías de telecomunicaciones; sin embargo, son diferentes en el sentido de que, en general, proporcionan servicios sólo a los empleados de la compañía que es propietaria de la red.

Este capítulo finaliza con una descripción de Internet, que es una red única en muchos sentidos: representa la influencia más poderosa en el desarrollo de las tecnologías de red en todo el mundo.

5.2 ESTRUCTURA GENERAL DE UNA RED DE TELECOMUNICACIONES

PALABRAS CLAVE: red de telecomunicaciones, estructura, equipo terminal de datos, red de acceso, troncal, red principal, centros de datos, punto de control del servicio, conmutador (PBX), información del usuario e información subsidiaria.

A pesar de las diferencias entre redes de computadoras, telefónicas, de televisión, de radio y de transmisión, existen características comunes en cuanto a su estructura. En general, cualquier red de telecomunicaciones cuenta con los componentes que siguen (figura 5.1):

- Equipo terminal de datos (probablemente conectado a la red)
- Redes de acceso
- Red troncal (o principal)
- Centros de datos o puntos de control del servicio

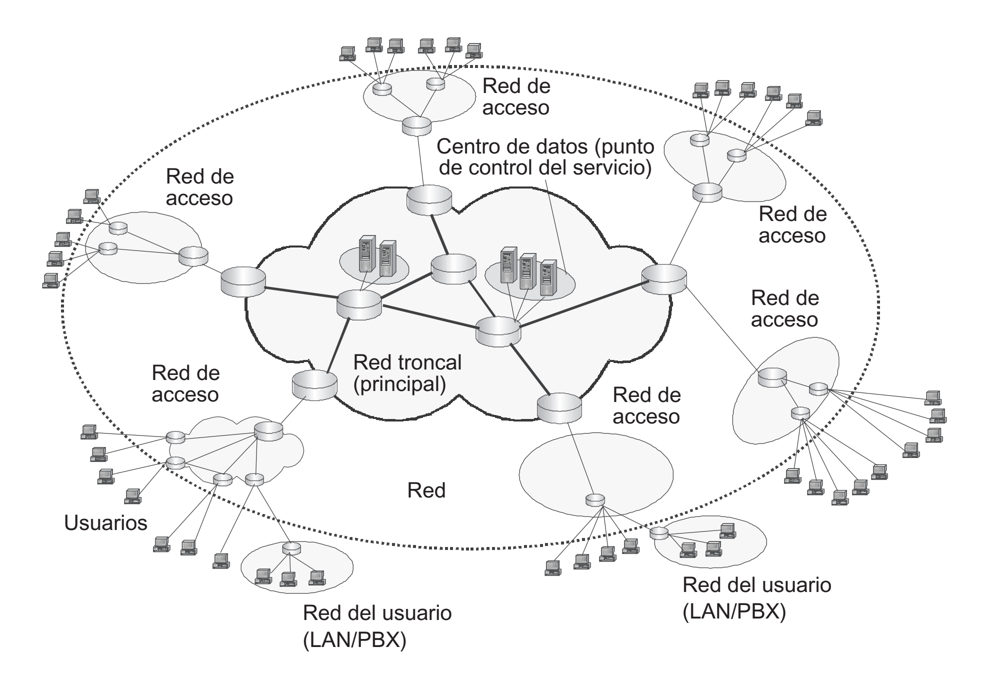


FIGURA 5.1 Estructura generalizada de una red de telecomunicaciones.

Tanto la red de acceso como la troncal están diseñadas con base en switches, cada uno de los cuales cuenta con varios puertos conectados a los puertos de los demás switches o interruptores a través de **enlaces de telecomunicaciones**.

5.2.1 Redes de acceso

Las **redes de acceso** forman la capa jerárquica más baja en una red de telecomunicaciones. Su propósito principal es la concentración de flujos de información que llegan a través de distintos tipos de enlaces provenientes del equipo del usuario, hacia un número relativamente pequeño de nodos de la troncal.

Cuando se trabaja con redes de computadoras, los nodos terminales representan computadoras; en las redes telefónicas, los nodos terminales están representados por aparatos telefónicos; y en las redes de radio o televisión lo están por los receptores de radio y televisión correspondientes. El equipo terminal de los usuarios finales puede conectarse para formar redes no incluidas en la red de telecomunicaciones, ya que dicho equipo es propiedad del usuario final y se localiza en sus instalaciones. Las computadoras de los usuarios finales están conectadas en forma de LAN; los teléfonos pueden estar conectados al **conmutador (PBX)**.

La red de acceso es una red regional caracterizada por una gran cantidad de ramificaciones. Al igual que las redes de telecomunicaciones, las de acceso pueden incluir varias capas. El dibujo de la figura 5.1 muestra dos de ellas. Los switches instalados en los nodos de las capas inferiores multiplexan la información que llega proveniente de múltiples canales de suscriptores, con frecuencia llamados loops locales y la transmiten a los switches de las capas superiores, los cuales a su vez la transfieren a los switches que forman la red troncal.

El número de capas de la red de acceso depende de su tamaño. Las redes de acceso pequeñas sólo tienen una capa, mientras que las más grandes generalmente cuentan con dos o tres capas.

5.2.2 Troncales

La **red troncal (principal)** conecta a diferentes redes de acceso y transmite tráfico en tránsito entre ellas, mediante el uso de enlaces de gran velocidad.

Los switches de la troncal pueden trabajar no sólo con enlaces de información entre los usuarios individuales, sino también con flujos de información agregada que transportan los datos de un gran número de conexiones de usuario. Como resultado de esto, la información que viaja a través de la troncal llega a la red de acceso del receptor, donde se demultiplexa y se conmuta, de tal forma que el puerto de entrada de cada usuario recibe solamente la información destinada a él.

EJEMPLO *Usted puede observar fácilmente que cualquier red carretera tiene la misma estructura jerárquica que la de una red de telecomunicaciones. Como regla general, los pueblos y las ciudades pequeñas están conectados mediante una infraestructura grande y ramificada de caminos locales. Dichos caminos son angostos y la intensidad de tráfico en ellos es baja, por lo que no es necesario construirlos con muchos carriles. Estos caminos conectan carreteras, las cuales son más anchas y, por lo tanto, en ellas se alcanzan velocidades más altas; a su vez, las carreteras conectan a supercarreteras. Esto refleja la intensidad de tráfico entre los pueblos pequeños y las regiones del país y hace que el tráfico de automotores sea más eficaz.*

5.2.3 Centros de datos

Los **centros de información** (o **de datos**) o **puntos de control de servicio (SCP)** brindan los servicios de información de la red. Dichos centros pueden almacenar dos tipos de información:

- Información del usuario, la cual es de gran interés para los usuarios finales de la red
- Información subsidiaria, que ayuda a brindar servicios a los usuarios finales

Algunos ejemplos de recursos de información son los portales en la web que contienen información de referencia, noticias, los datos de las tiendas de Internet, etc. En las redes telefónicas, dichos centros proporcionan servicios tales como llamadas de emergencia (es decir, llamadas a la policía o a un servicio de ambulancias) y los servicios de consulta de organizaciones, como estaciones de ferrocarril, aeropuertos y tiendas.

Los centros de información, que almacenan recursos del segundo tipo, incluyen varios sistemas para la autentificación y autorización de usuarios que el propietario de la red utiliza para verificar los derechos de los usuarios a servicios específicos, sistemas de cobro que calculan el pago de servicios en redes comerciales, bases de datos de las cuentas de los usuarios que almacenan cuentas de usuario y contraseñas, y listas de servicios a las que está suscrito cada usuario. En las redes telefónicas existen SCP centralizados, donde las computadoras corren programas para el manejo de las llamadas telefónicas de los usuarios, como llamadas a servicios de consulta de organizaciones comerciales sin cobro (servicios 1-800) o llamadas realizadas durante las encuestas telefónicas.

Como es natural, cada tipo de red tiene características específicas; sin embargo, su estructura generalmente corresponde a la descrita con anterioridad. Al mismo tiempo, según los objetivos y el tamaño de la red, algunos componentes de la estructura generalizada pueden o no estar presentes. Por ejemplo, en una LAN pequeña no existen muchas redes de acceso o troncales, ya que éstas se hallan fusionadas en una estructura relativa-

mente simple. Como regla, en una red corporativa no existe sistema de cobro, puesto que la compañía proporciona servicios sin cobro a sus empleados. Los centros de datos pueden adolecer de redes telefónicas. En el caso de las redes de televisión, la red de acceso tiene la apariencia de una red de distribución, ya que los flujos de información en dichas redes son unidireccionales: de la red hacia los suscriptores.

5.3 REDES DE TELECOMUNICACIONES DE LARGA DISTANCIA

PALABRAS CLAVE: telecomunicaciones, prestador de servicios de larga distancia, proveedor de servicios, red corporativa, servicios de telefonía, servicios de redes de computadora, servicios de transporte, servicios de información, servicios interactivos, servicios de difusión, clientes individuales masivos, clientes corporativos, infraestructura, RBOC, BOC, CLEC, ILEC, portadores de servicios entre centrales (IXC), puntos de presencia (POP), portadores locales tradicionales, prestadores de servicios regionales, competitivos, nacionales e internacionales.

Como ya se mencionó, una de las características más importantes de la clasificación de las redes es la gama de usuarios a la que la red brinda servicios. Las redes que pertenecen a las compañías de larga distancia (proveedoras del servicio) proporcionan servicios públicos, mientras que las redes corporativas solamente dan servicio a los empleados de la compañía que es propietaria de la red.

Prestador de servicios de telecomunicaciones es un término tradicional que se refiere a una compañía especializada que construye redes de telecomunicaciones para brindar servicios públicos, es propietaria de dicha red y se encarga de su operación.

El prestador de servicios de telecomunicaciones brinda servicios comerciales a sus clientes de acuerdo con contratos de servicio.

Un prestador de servicios de telecomunicaciones difiere de otro de las formas siguientes:

- Conjunto de servicios ofrecidos
- Territorio en el que brinda dichos servicios
- Tipo de clientes hacia los que están orientados los servicios
- Infraestructura que tiene el prestador de servicios de telecomunicaciones: enlaces de comunicaciones, equipo de conmutación, servidores de información, etcétera
- Relación con el monopolio en el campo

5.3.1 Servicios

Los prestadores de servicios de telecomunicaciones modernos generalmente ofrecen servicios de varios tipos, por ejemplo: servicios de telefonía y servicios de Internet. Los **servicios** pueden clasificarse en varias capas y en grupos. La figura 5.2 muestra solamente algunas de las capas y grupos principales; sin embargo, aun este patrón incompleto muestra el rango de servicios modernos de telecomunicaciones y la complejidad de sus interrelaciones. Los servicios de las capas superiores están basados en los servicios de las capas inferiores. Los grupos de servicios están combinados de acuerdo con el tipo de redes que los ofrecen: redes telefónicas o de computadoras. Con el fin de obtener un patrón más completo, uno puede complementar esta figura con los servicios proporcionados por las redes de radio y televisión.

Servicios combinados: • Telefonía IP • Mensajería unificada • Videoconferencia	
Servicios de telefonía: • Acceso a servicios por demanda • Correo de voz • Redirección de llamadas • Conexión de dos suscriptores	**Servicios de las redes de computadoras:** • Redes privadas virtuales • Portales de información (www) • Correo electrónico • Acceso a Internet • Conexión LAN
Servicios de líneas conmutadas	

FIGURA 5.2 Clasificación de los servicios proporcionados por la red de telecomunicaciones (las áreas sombreadas corresponden a los servicios convencionales de los proveedores de servicios de telecomunicaciones).

Los servicios de líneas arrendadas son los servicios de la capa inferior, pues los clientes que gozan de este servicio tienen que construir su infraestructura de red con base en estas líneas arrendadas. Dichos clientes deben instalar switches telefónicos o switches de redes de conmutación de paquetes, antes de que puedan obtener los beneficios de este servicio. En general, los clientes que se suscriben a dicho servicio son prestadores de servicios de telecomunicaciones que no poseen enlaces de comunicaciones o grandes compañías que construyen redes corporativas privadas con base en estas líneas arrendadas. Las redes corporativas se estudiarán en la siguiente sección.

La capa siguiente comprende dos grandes grupos de servicios: **servicios de telefonía** y **servicios de redes de computadoras**. Los servicios de telefonía y de líneas arrendadas representaron durante mucho tiempo un conjunto tradicional de servicios.

Los servicios de redes de computadoras aparecieron mucho después que los de telefonía y, aun en la actualidad, están muy atrás respecto a los servicios telefónicos convencionales en cuanto al nivel de ingresos. Sin embargo, la mayoría de los prestadores de servicios de telecomunicaciones proporcionan servicios de redes de computadoras, ya que éstos tienen excelentes prospectos y están significativamente adelante de los servicios convencionales en cuanto a tasa de crecimiento. Si se habla en cantidades absolutas, el tráfico de datos ha excedido al de voz; no obstante, las bajas tarifas de los servicios de transmisión de datos evitan que compitan con los servicios tradicionales en términos de ingresos.

Cada una de las capas de servicio descritas con anterioridad puede dividirse en subcapas; por ejemplo, con base en el servicio de acceso a Internet (conexión de transporte de una computadora o LAN a Internet), el prestador de servicios de telecomunicaciones debe ofrecer al cliente la posibilidad de organizar una VPN, asegurarse contra otros usuarios de Internet, o crear el portal web del cliente, hospedándolo dentro de la red del proveedor del servicio.

En la actualidad, la capa superior de la jerarquía de servicios está ocupada por servicios combinados implementados con base en la operación coordinada de redes de computadoras y telefónicas. La telefonía IP internacional, que ha acaparado a un gran número de usuarios respecto a la telefonía internacional convencional, es un ejemplo apabullante de dichos servicios.

Los servicios combinados son resultado directo de la convergencia de las redes, así como de la fuerza que impulsa este proceso.

Los servicios también pueden clasificarse mediante la aplicación de los principios de los **servicios de transporte** o **servicios de información**. De acuerdo con esta clasificación, las conversaciones telefónicas son un servicio de transporte, ya que los prestadores de servicios de telecomunicaciones entregan tráfico de voz de suscriptor a suscriptor. Los servicios de consulta de la red telefónica hacia sitios web representan un ejemplo de servicios de información.

Este tipo de diferencias en cuanto a los servicios proporcionados por las compañías de telecomunicaciones se refleja en las diferencias de sus nombres. Las compañías tradicionales cuyo campo principal de actividades de negocios siempre han sido los servicios de telefonía y los servicios de líneas arrendadas (es decir, servicios de transporte) se conocen con el nombre de **prestadores de servicios de telecomunicaciones**. El término **prestador de servicios** (SP, por sus siglas en inglés) se hizo muy popular con el crecimiento explosivo de Internet y su servicio WWW (es decir, un servicio de información).

Los servicios pueden ser diferenciados no solamente por el tipo de información que proporcionan, sino también por el nivel de interactividad. Así, las redes telefónicas proporcionan **servicios interactivos**, ya que dos suscriptores participan en la conversación (o varios de ellos si se trata de una conferencia) e interactúan alternadamente. Las redes de computadoras brindan servicios similares a estos, en los que los usuarios pueden observar el contenido del sitio mientras contestan las preguntas de la forma de registro o, por ejemplo, mientras practican con juegos interactivos.

Por otro lado, las redes de radio y las de televisión proporcionan **servicios de difusión (broadcast)**: la información sólo se transmite en una dirección —de la red a los suscriptores— de acuerdo con un arreglo punto a multipunto.

5.3.2 Clientes

La audiencia que consume servicios de información y comunicaciones puede dividirse en dos grandes grupos: **clientes individuales masivos** y **clientes corporativos**.

En el primer grupo, las instalaciones del cliente son privadas y los clientes son huéspedes que necesitan servicios básicos como las comunicaciones telefónicas, televisión, radio y acceso a Internet. Para ellos el factor más importante es la economía del servicio: una renta mensual baja, la posibilidad de usar dispositivos terminales estándar, como teléfonos, aparatos de televisión o PC; y la posibilidad de usar el cableado existente, como cables de par trenzado o coaxial para televisión. No es muy probable que se presente un uso masivo de dispositivos terminales sofisticados, difíciles de usar y costosos (como televisiones computarizadas o teléfonos IP) hasta que su costo sea comparable con el de las televisiones y teléfonos convencionales.

Además del factor económico, dichos dispositivos deben soportar una interfase de usuario sencilla que no requiera que el usuario tenga que asistir a cursos especiales para manejarlos. El cableado existente en la mayoría de los edificios también representa una limitante para el acceso a Internet y a nuevos servicios proporcionados por las redes de computadoras, ya que inicialmente no fue diseñado para la transmisión de datos. La instalación de un cable de alta calidad (por ejemplo, fibra óptica) es costosa. Debido a esto, los usuarios domésticos suelen conectarse a Internet mediante el uso de módems conmutados de baja velocidad; sin embargo, hoy en día han cobrado mucha popularidad nuevas tecnologías, como la línea de

suscripción digital (DSL), la cual permite la transmisión de datos a través de líneas telefónicas existentes a velocidades significativamente más rápidas que los módem convencionales. Además, existen tecnologías de acceso que utilizan redes existentes de televisión por cable para la transmisión de datos.

Los **clientes corporativos** por lo general son organizaciones o empresas. Los negocios pequeños no son significativamente distintos de los clientes individuales, si usted considera el conjunto de servicios que se requieren. Como regla general, éstos son los mismos servicios de telefonía básica y televisión y el acceso conmutado a recursos de información de Internet. La única diferencia reside en la cantidad de números telefónicos que se necesitan (generalmente dos o más).

Las grandes corporaciones formadas por varios departamentos geográficamente distribuidos, o sucursales que emplean usuarios móviles que a menudo trabajan en casa (trabajadores a distancia o teletrabajadores), necesitan un conjunto de servicios más amplio. Entre dichos servicios se debe incluir el de *VPN*. El portador de servicios que proporciona dicho servicio crea a la compañía la ilusión de que todos sus departamentos y sucursales están conectados mediante una red privada (es decir, el cliente es el dueño y administra la totalidad de la red). La red del prestador de servicios se utiliza para estos propósitos y es una red pública que transmite, de forma simultánea, los datos de un gran número de clientes.

En la actualidad, los clientes corporativos a menudo requieren servicios no sólo de transporte, sino también de información; por ejemplo, dichos clientes transfieren sus sitos web y bases de datos a las instalaciones del proveedor del servicio, al cual se le delega la responsabilidad de mantener su operación y asegurar un acceso rápido a estos recursos de información de los empleados de la corporación y, posiblemente, de otros suscriptores de la red del prestador de servicios.

5.3.3 Infraestructura

Infraestructura: además de las razones subjetivas que influyen en la formación de los servicios proporcionados por el prestador de servicios de telecomunicaciones, los factores técnicos desempeñan un papel muy importante. Por lo tanto, para proporcionar servicios de líneas arrendadas, el prestador de servicios debe contar con redes de transmisión a su disposición; por ejemplo, considere SDH o una red de conmutación de circuitos como ISDN. Para proporcionar servicios de información es necesario crear sitios web conectados a Internet, de tal forma que los usuarios de Internet puedan acceder a ella.

Si el prestador de servicios no posee la infraestructura necesaria para ofrecer un servicio específico, es posible utilizar los servicios de otro prestador de servicios. Dichos servicios, combinados con algunos elementos de la infraestructura propia del portador de servicios, hacen posible construir el servicio que el cliente necesita. Por ejemplo, un prestador de servicios de telecomunicaciones contratado para construir un sitio web público de comercio electrónico no tendrá su propia red IP conectada a Internet. Para proporcionar este servicio, es suficiente crear el contenido y colocarlo en la computadora de otro proveedor de servicios cuya red esté conectada a Internet. El arrendamiento de los enlaces físicos de comunicaciones para crear una red telefónica o de computadoras es otro ejemplo de proporcionar servicios cuando no se cuenta con alguno de los elementos de la infraestructura de hardware o software. El prestador de servicios que a su vez brinda servicios a otros prestadores de servicios de telecomunicaciones se llama proveedor de proveedores de servicio.

En la mayoría de los países, los prestadores de servicios de telecomunicaciones deben obtener licencias con el fin de brindar tipos específicos de servicios de estructuras guber-

namentales; empero, la situación no fue siempre así. En prácticamente todos los países, los prestadores de servicios representaban un monopolio en el mercado de los servicios de telecomunicaciones a nivel nacional. En la actualidad, el proceso de eliminación de monopolios en los servicios de telecomunicaciones se lleva a cabo a pasos agigantados.

ELIMINACIÓN DE MONOPOLIOS EN EL MERCADO DE LAS TELECOMUNICACIONES EN ESTADOS UNIDOS

Como resultado, los monopolistas perdieron sus privilegios. En algunos casos fueron fragmentados por la fuerza en compañías más pequeñas; por ejemplo, en Estados Unidos, AT&T tuvo el monopolio para brindar servicios de telefonía local y de larga distancia hasta 1984. En dicho año, de acuerdo con una decisión en la corte, AT&T se fragmentó en partes más pequeñas, siendo la más importante AT&T Long Lines, a la cual se permitió proporcionar servicios de larga distancia solamente y 23 compañías operativas Bell (BOC, por sus siglas en inglés), las cuales tuvieron el derecho a proporcionar servicios telefónicos en pequeña escala solamente. Para brindar servicios a una escala regional, las BOC se unieron en siete BOC regionales (RBOC).

Los monopolistas nacionales, despojados de sus privilegios y divididos en pequeñas compañías, tuvieron que competir para ganar clientes con nuevos prestadores de servicios que aparecieron en los mercados de servicio local, así como en mercados regionales y en el mercado de larga distancia. A dichos prestadores de servicios por lo general se les llama competencia. En Estados Unidos, la evolución de la competencia del mercado de los servicios de telecomunicaciones se aceleró en 1996, cuando el Congreso aprobó el Acta de Telecomunicaciones y eliminó las restricciones que tenían los prestadores de servicios de telecomunicaciones, que hacían que sólo pudieran proporcionar servicios en un segmento de mercado, ya sea en el de los servicios de larga distancia regional o en el de los servicios de telefonía local. En la actualidad, los proveedores de servicios de intercambio local competitivos (CLEC) en Estados Unidos son numerosos, como también lo eran los monopolistas locales anteriores: proveedores de servicios de intercambio local de incumbencia (ILEC). La competencia no es menos intensa en el mercado regional y de larga distancia en la Unión Americana, donde existe un gran número de prestadores de servicio, conocidos como proveedores entre centrales (IXC). Esta terminología es importante debido a que a veces se utiliza para describir soluciones a proyectos y tecnologías. Por lo tanto, el tipo de prestador de servicios de telecomunicaciones (IXC, CLEC o ILEC) marca su posición dentro de un sistema de portadores y prestadores de servicios, así como de los servicios específicos proporcionados.

5.3.4 Cobertura

De acuerdo con el territorio abarcado por sus servicios, los prestadores de servicios se dividen en locales, regionales, nacionales e internacionales.

Los **prestadores de servicios locales** operan dentro de una ciudad o área rural y los **prestadores de servicios locales convencionales** (ILEC, en la terminología estadounidense) son los operadores de las redes telefónicas en las ciudades que cuentan con toda la infraestructura adecuada de transporte: loops locales que conectan las instalaciones de los suscriptores (departamentos, edificios y oficinas) con una central telefónica local. Los switches telefónicos y los enlaces de comunicaciones están instalados entre ambos. En la actualidad, además de los prestadores de servicios convencionales, están los **competitivos** (CLEC), quienes a menudo ofrecen nuevos tipos de servicios, relacionados con Internet principalmente. A veces, éstos también compiten con los prestadores de servicios tradicionales en el sector telefónico.

A pesar de la eliminación de monopolios en las telecomunicaciones, los prestadores de servicios locales convencionales siguen siendo los propietarios de los loops locales.

En esas condiciones de derechos no equitativos, los prestadores de servicios locales competitivos con frecuencia tienen problemas para operar sus negocios. Esto les deja varias opciones. Primero, pueden especializarse en ofrecer servicios adicionales relacionados solamente con la transmisión y procesamiento de datos: proveer acceso a Internet, hospedar los recursos de información de sus clientes, etc. Para organizar el acceso del suscriptor a estos recursos, dichos prestadores de servicio tienen que firmar contratos con los prestadores de servicios tradicionales que envían el tráfico del suscriptor conectado a su red hacia la red del prestador de servicios competitivos. En este caso, la especialización natural de los prestadores de servicios es evidente, ya que cada uno se especializa en el área para la cual es más apropiada la infraestructura disponible de la compañía. En dichas condiciones, la cooperación motiva la aparición de nuevos servicios. Segundo, los prestadores de servicios competitivos pueden arrendar loops locales a los prestadores de servicios convencionales. Usualmente, los prestadores de servicios convencionales se oponen a hacer eso, aunque la legislación en algunos países fomenta o incluso obliga a que se haga así. La tercera opción es construir sus propias redes de loops locales. Aquí, el prestador de servicios competitivos tiene dos opciones: loops locales alámbricos o inalámbricos. Si se considera el número de residencias privadas, la dificultad de instalar cables y la necesidad de comprar una licencia a las autoridades locales, todo ello hace que la versión alámbrica sea con mucha frecuencia una opción poco eficaz desde el punto de vista económico. Esta circunstancia ha generado un gran interés en las soluciones inalámbricas, las cuales están creciendo a pasos agigantados.

Los **prestadores de servicios regionales** y **nacionales** que ofrecen servicios en territorios grandes cuentan con la infraestructura de transporte apropiada a su disposición. Los prestadores de servicios convencionales de esta envergadura transmiten tráfico telefónico entre los conmutadores de los prestadores de servicio locales. En general, éstos son propietarios de grandes centrales de tránsito conectadas a través de enlaces de comunicaciones de alta velocidad. Dichas compañías, por lo general, son proveedores de proveedores de servicio. Entre sus clientes están prestadores de servicios locales o corporaciones grandes con sucursales y departamentos en varias ciudades de una región específica o incluso en todo un país. Su propia infraestructura avanzada de transporte permite que dichos prestadores de servicios brinden servicios de larga distancia y transmitan grandes volúmenes de información sin necesidad de procesamiento.

Los servicios de los prestadores de servicio internacional pueden abarcar varios países. Entre ellos, los más conocidos son Cable & Wireless, Global One e Infonet, los cuales son propietarios de troncales que a menudo abarcan varios continentes. Con frecuencia, dichos prestadores de servicio operan en colaboración con prestadores de servicios nacionales, utilizando sus redes de acceso para entregar la información a sus clientes.

5.3.5 Relación entre los diferentes tipos de prestadores de servicios

La figura 5.3 muestra la relación entre los diferentes tipos de prestadores de servicios y entre sus redes. Esta figura también muestra dos tipos de clientes: individuales y corporativos. Tenga en cuenta que cada cliente, por lo común, requiere dos tipos de servicios: servicios telefónicos y servicios de datos. Como regla general, los clientes individuales tienen teléfonos y computadoras en sus casas. Los clientes corporativos poseen sus propias redes: redes telefónicas soportadas por PBX o LAN para la transmisión de datos, construidas con base en los switches de la compañía.

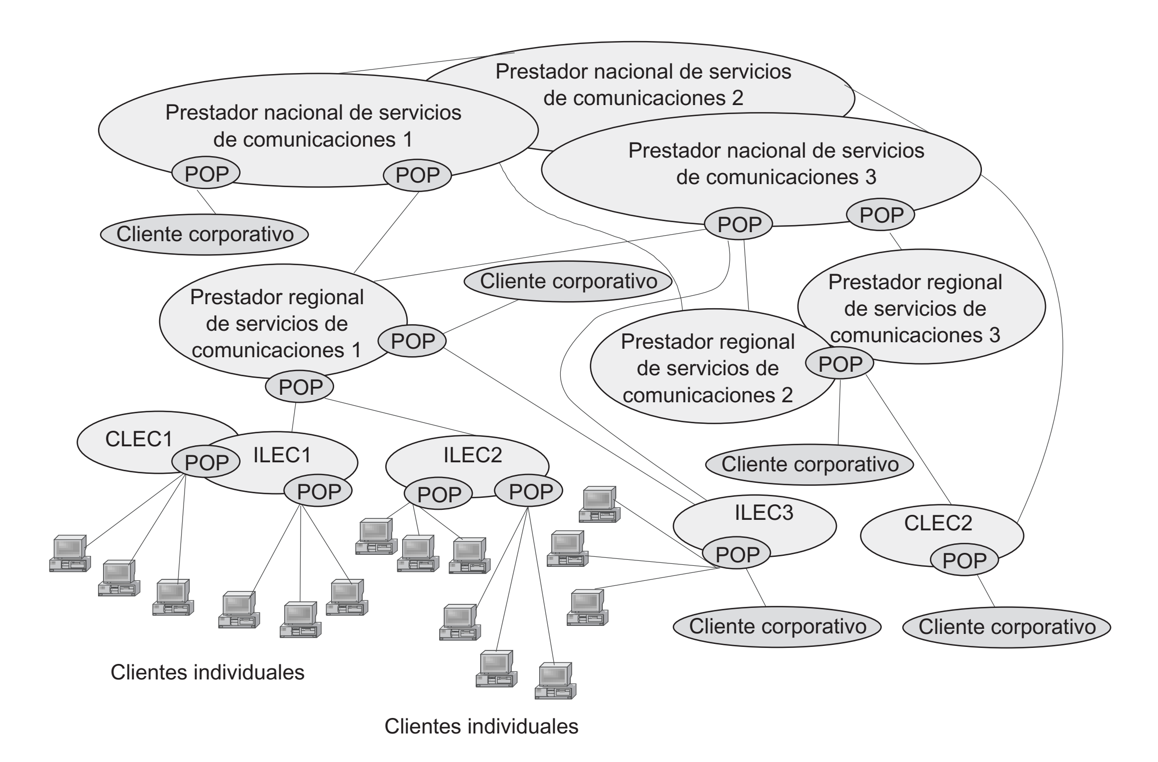


FIGURA 5.3 Interrelaciones entre los diferentes tipos de prestadores de servicios de comunicaciones.

Para conectar el equipo del cliente, los prestadores de servicios disponen de **puntos de presencia (POP)**, edificios o instalaciones donde éstos colocan el equipo de acceso para conectar un gran número de loops locales de sus clientes. A veces, estos POP se llaman centrales telefónicas, un término utilizado por los prestadores de servicios telefónicos. Los suscriptores se conectan a los POP de los prestadores de servicios locales; dichos prestadores o los clientes corporativos grandes, quienes necesitan acceso a alta velocidad y cobertura para conectar sus oficinas y sucursales en diferentes ciudades y países, se conectan a los POP de los prestadores de servicios de más alto nivel.

Dado que el proceso de convergencia todavía no crea una red unificada para dar servicio a todos los tipos de tráfico, cada red proveedora en esta figura representa dos redes: la telefónica y la de datos.

Como puede observarse en la figura 5.3, en el mundo competitivo actual de las telecomunicaciones no existe una jerarquía estricta de los proveedores de servicios. La interrelación entre ellos y sus redes puede ser complicada. Por ejemplo, la red CLEC2 tiene una conexión directa no solamente al carrier3 regional, como lo requiere la jerarquía, sino también al carrier3 nacional. Esto puede deberse a que la compañía ofrece servicios más baratos para la transmisión de tráfico internacional que el carrier3 regional; además, como lo muestra la figura 5.3, no todos los proveedores de servicio tienen una infraestructura de transporte (por ejemplo, CLEC1). La CLEC1 ofrece a menudo servicios de información adicionales (por ejemplo, proporciona video por demanda a los suscriptores de ILEC1 o desarrolla y soporta sus páginas de Internet). Dichos prestadores de servicios también colocan su equipo (por ejemplo, sus servidores de video) en el POP u otro prestador de servicios, como se muestra.

5.4 REDES CORPORATIVAS

PALABRAS CLAVE: red departamental, red corporativa, red en un edificio o en un campus, red de grupos de trabajo, redes corporativas y subred.

Una **red corporativa** es aquella cuyo objetivo principal consiste en proporcionar soporte a la operación de la compañía específica que la posee. Los usuarios de una red corporativa son los empleados de dicha compañía en particular. En contraste con las redes proveedoras de servicios de telecomunicaciones, las redes corporativas no ofrecen servicios a terceras organizaciones ni a usuarios externos.

Aunque una red que sea propiedad de una compañía de cualquier tamaño puede considerarse formalmente una red corporativa, este término se utiliza en general para las redes que son propiedad de grandes empresas, las cuales tienen departamentos o sucursales en diversas ciudades y, probablemente, en varios países. Por lo tanto, una red corporativa suele ser una interred compuesta por LAN y WAN.

La estructura de una red corporativa generalmente corresponde a la de la red de telecomunicaciones que se consideró con anterioridad; sin embargo, existen diferencias. Por ejemplo, las LAN que conectan a los usuarios finales en este caso están integradas en la red corporativa. Además, los nombres de las divisiones estructurales de la red corporativa generalmente reflejan no sólo la cobertura geográfica, sino también la estructura organizacional de la compañía. Por lo tanto, es común dividir a las redes corporativas en subredes de departamentos o grupos de trabajo, redes de edificios o campus y una troncal.

5.4.1 Redes departamentales

Las **redes departamentales** son utilizadas por grupos de empleados relativamente pequeños que trabajan en el mismo departamento de la compañía. Dichos empleados resuelven problemas comunes o llevan a cabo tareas en conjunto al trabajar en diferentes departamentos, como contabilidad o mercadotecnia. Se supone, en general, que un solo departamento puede tener de 100 a 150 empleados. Las redes departamentales consisten en una LAN cuya cobertura abarca todas las instalaciones que posee determinado departamento. Según la situación, éstas pueden abarcar varias oficinas o un piso completo de un edificio.

El objetivo principal de una red departamental es compartir recursos locales, como aplicaciones, datos, impresoras láser y módems. En general, las redes departamentales cuentan con uno o dos servidores de archivos, algunos concentradores y switches y no tienen más de 30 usuarios (figura 5.4). La mayor parte del tráfico de la compañía está en dichas redes. Las redes departamentales generalmente se basan en una sola tecnología de red: Ethernet (o varias tecnologías de esa misma familia, como Ethernet, Fast Ethernet o la menos común Gigabit Ethernet), *Token Ring* o FDDI. Dichas redes suelen utilizar no más de dos tipos de sistemas operativos.

Las labores relacionadas con el mantenimiento de la red a nivel de departamento son relativamente sencillas: agregar nuevos usuarios, eliminar los efectos de fallas sencillas e instalar nuevos nodos y nuevas versiones de productos de software. Las tareas de administración y mantenimiento de dichas redes pueden delegarse a un empleado que se dedique a las actividades administrativas en tiempo parcial. Con frecuencia, el administrador de la red

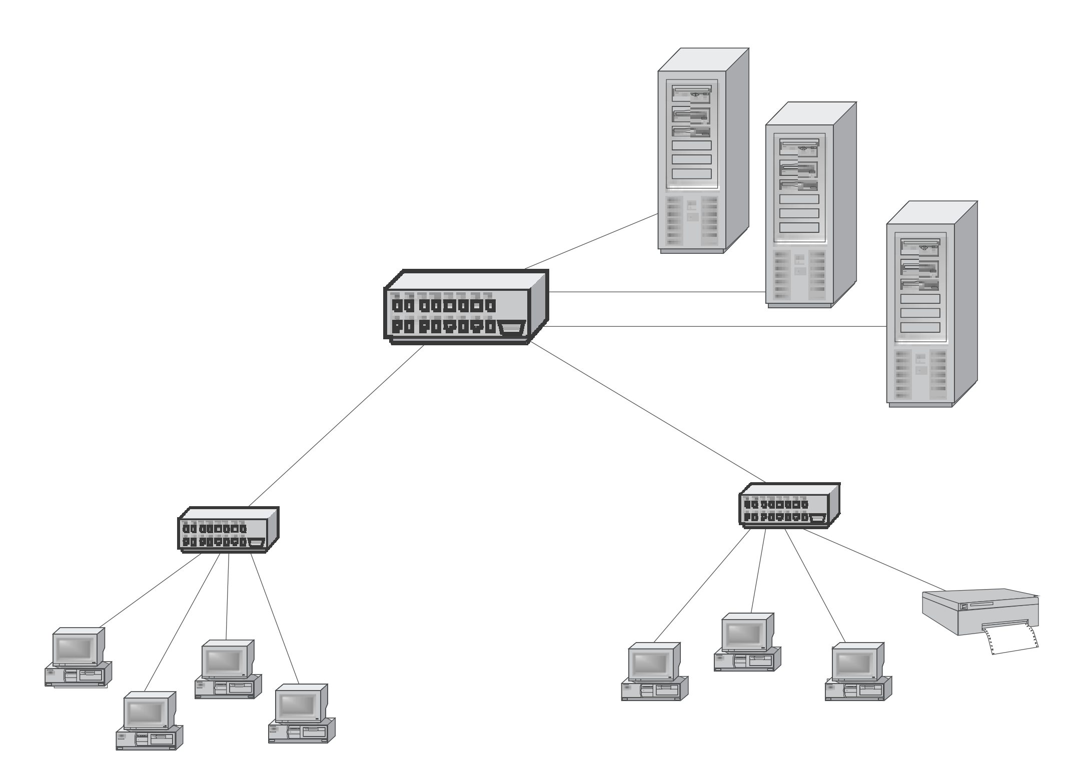


FIGURA 5.4 Ejemplo de una red departamental.

departamental no es un experto; sin embargo, tiene una mejor comprensión del hardware y el software de las computadoras que los demás empleados. Su trabajo principal consiste en llevar a cabo funciones administrativas.

Existe otro tipo de red similar a la departamental: la **red de grupo de trabajo**. Estas también son redes muy pequeñas, que constan de 10 a 20 computadoras. Las redes de grupos de trabajo, en la práctica, no son diferentes de las redes departamentales que se acaban de estudiar. Algunas propiedades como la simplicidad y la homogeneidad de la red son las más evidentes en las redes de grupos de trabajo.

Las redes de grupos de trabajo a menudo usan tecnologías LAN que se basan en un medio compartido. A medida que el nivel jerárquico de la red es mayor, el medio compartido se utiliza con menor frecuencia; en lugar de emplearlo se reemplaza por LAN conmutadas.

Las redes departamentales pueden estar ubicadas como parte de la red de un edificio o de un campus. También pueden representar la red de una oficina remota. Una red departamental se conecta a la red de un edificio o campus mediante tecnologías LAN; en la actualidad, ésta probablemente será una de las representantes de la familia Ethernet. La red de oficina remota se conecta directamente a la troncal mediante el uso de las tecnologías WAN (por ejemplo, *Frame Relay*).

5.4.2 Redes en edificios o en campus

Las **redes en edificios o en campus** se conectan a diferentes redes propiedad de varios departamentos de la misma compañía, ubicados en un edificio independiente o en un área de varios kilómetros cuadrados (figura 5.5). En la construcción de dichas redes se utilizan tecnologías LAN, ya que sus características funcionales son suficientes para asegurar esta cobertura.

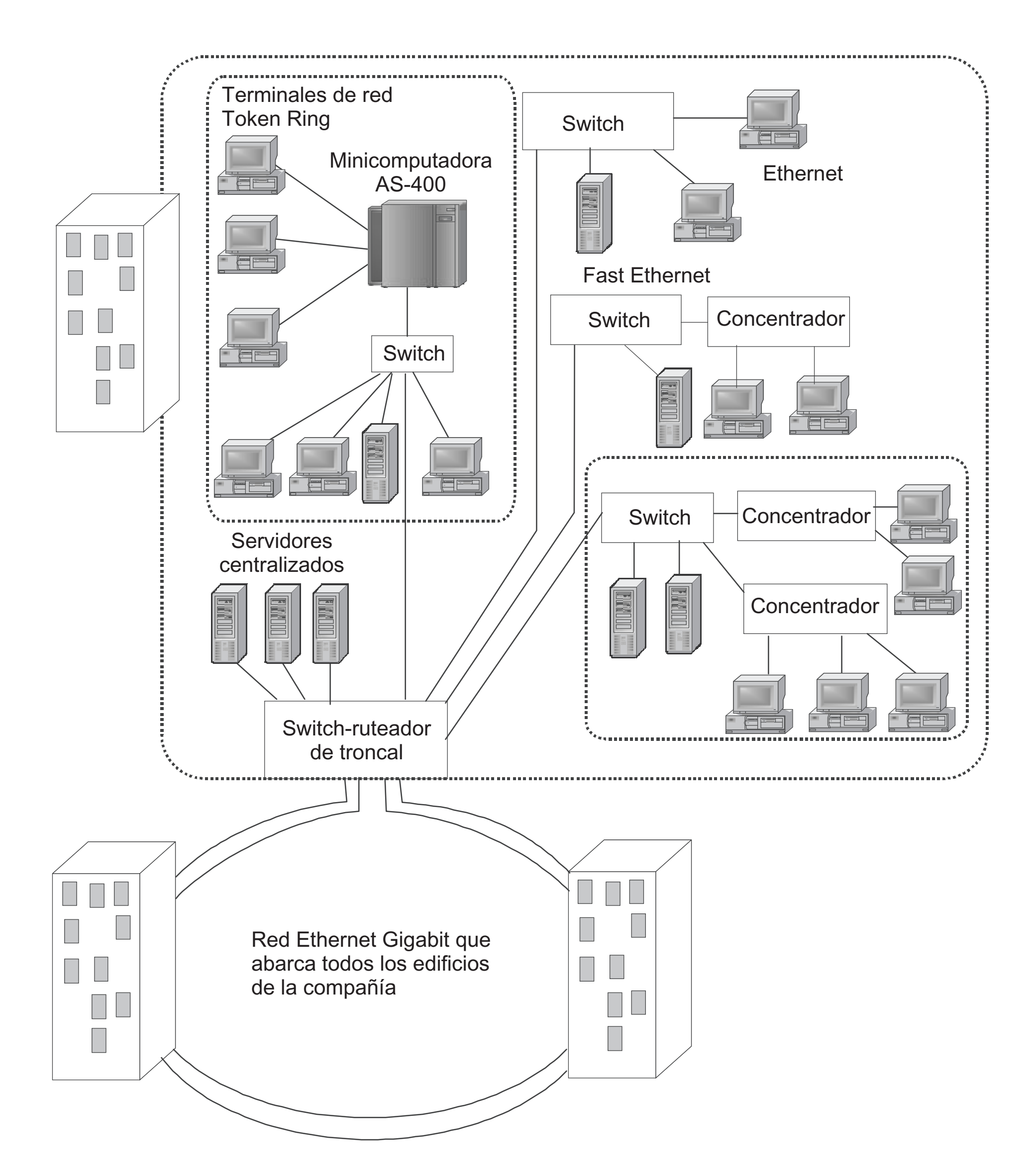


FIGURA 5.5 Ejemplo de una red de campus.

Normalmente, una red dentro de un edificio o un campus se construye de acuerdo con el principio jerárquico (es decir, tiene su propia troncal, la cual generalmente se basa en tecnología Ethernet Gigabit). Las redes de grupos de trabajo y departamentos conectadas a esta troncal se basan por lo general en Fast Ethernet o Ethernet. La troncal Ethernet Gigabit prácticamente está siempre conmutada, aunque existe una variante de esta tecnología que se basa en un medio compartido.

Entre los servicios que brinda esta red se encuentran la conectividad entre redes departamentales y el acceso a bases de datos de la compañía, servidores de fax, módem rápidos e impresoras. Como consecuencia, los empleados de cada departamento pueden acceder a algunos archivos y otros recursos de las redes de otros departamentos. El acceso independiente a las bases de datos corporativas es un servicio de gran importancia que ofrecen las redes en campus.

Los problemas respecto a la integración de hardware y software heterogéneo comienzan a surgir solamente a nivel de los campus. Los tipos de computadoras, sistemas operativos de red y equipo de red pueden ser muy diferentes en cada departamento; de aquí que las redes de campus son difíciles de administrar y controlar. Con mucha frecuencia, las redes de esta escala son redes interconectadas que se basan en la tecnología IP.

5.4.3 Redes corporativas

Las **redes corporativas** se distinguen por el hecho de que los servicios de información están en un primer plano. Estas redes no pueden limitarse solamente a los servicios de transporte. En contraste con las redes proveedoras de servicios de telecomunicaciones, las cuales pueden o no proporcionar servicios de información (ya que las computadoras del usuario final están fuera de los límites de su responsabilidad), las redes corporativas no pueden darse el lujo de proporcionar dichos servicios. Tanto las computadoras de escritorio de los usuarios finales como los servidores son partes integrales de cualquier red corporativa. Los diseñadores y el personal de soporte involucrados en el mantenimiento de las redes de este tipo deben tener en cuenta esto. Se puede decir que las redes corporativas son un ejemplo de redes de información y comunicación, en las que dos tipos de servicios están uno a la par del otro. Las redes corporativas pueden representarse como islas LAN que fluyen en el ambiente de las telecomunicaciones.

Otra característica de las redes corporativas es su escala. Las redes departamentales y las redes a nivel edificio rara vez se llaman corporativas, aunque esto es formalmente válido. En general, el término *corporativo* se utiliza para designar una red que comprende un gran número de redes departamentales o a nivel edificio ubicadas en diferentes ciudades y conectadas entre sí mediante enlaces WAN.

La estructura de la red corporativa no es, en principio, diferente de la general que se muestra en la figura 5.1. Las tecnologías WAN se utilizan para conectar LAN empresariales, que pueden ser redes de grupo de trabajo, departamentales o de edificio/campus. Dichas redes consisten en la *red troncal* y la *red de acceso*. Las corporaciones usan las mismas tecnologías WAN como proveedores de servicios de telecomunicaciones: ATM o Frame Relay. La tecnología IP se utiliza comúnmente para conectar las LAN y WAN a la red corporativa.

El número de usuarios y computadoras de una red corporativa puede ser del orden de miles, mientras que el número de servidores puede ser de cientos. Las distancias entre redes que abarcan regiones distantes pueden ser tan grandes, que el uso de enlaces WAN sea obligado (figura 5.6). Para conectar LAN distantes y computadoras independientes a redes corporativas, se pueden utilizar varias herramientas de telecomunicaciones, entre las que se incluyen circuitos de redes de transmisión, canales de radio y comunicaciones satelitales.

Un atributo necesario de dichas redes corporativas complejas es un alto grado de heterogeneidad. Es imposible satisfacer los requerimientos de múltiples usuarios que utilicen software y hardware del mismo tipo. Una red corporativa emplea diversos tipos de computadoras —que pueden variar desde equipos grandes hasta PC—, varios tipos de sistemas operativos y una amplia gama de aplicaciones. Las partes heterogéneas de las redes corporativas deben trabajar como si fueran una sola, proporcionando a los usuarios un acceso apropiado y sencillo a todos los recursos que puedan requerir.

La llegada de las redes corporativas es un buen ejemplo de un postulado filosófico bien conocido respecto a una transición de cantidad a calidad. Cuando se conectan redes independientes de una compañía grande distribuida geográficamente para formar una sola red, la mayoría de las características cualitativas de la interred exceden el umbral crítico, después

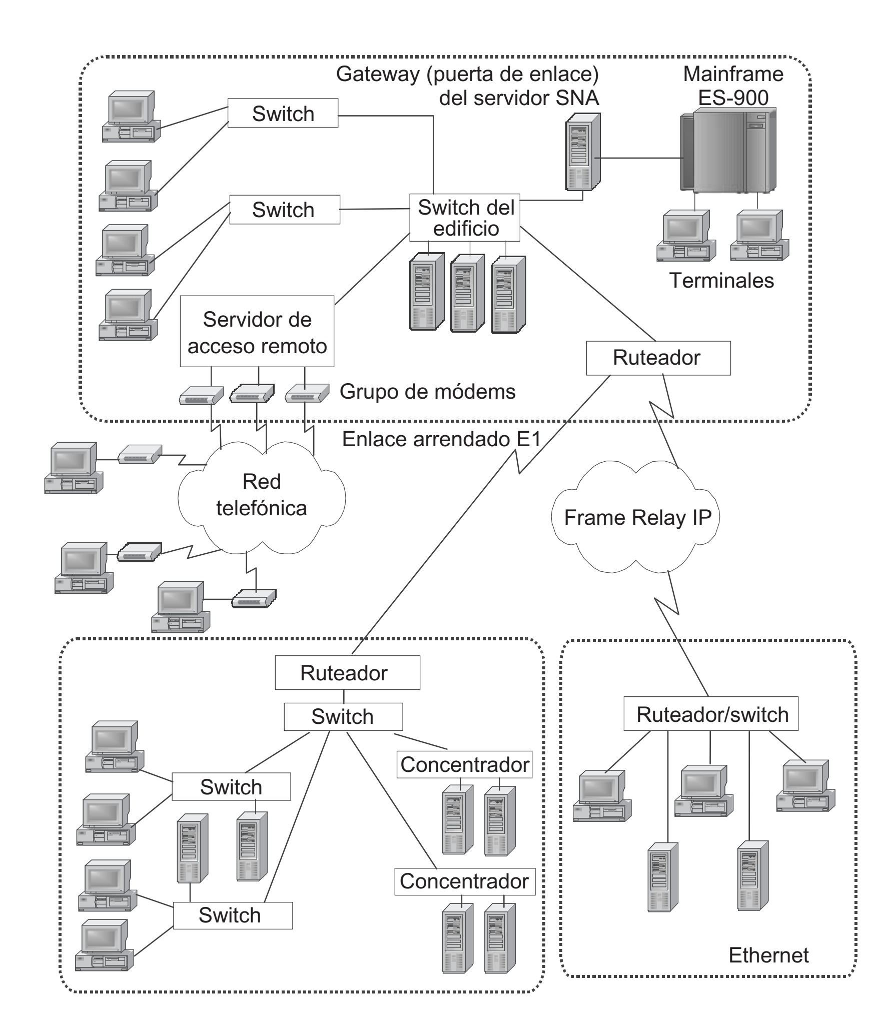


FIGURA 5.6 Ejemplos de una red corporativa.

del cual ésta adquiere nuevas características cualitativas. En estas condiciones, los métodos y formas existentes de resolver problemas típicos de redes pequeñas son inaplicables. Los problemas que eran de pequeña escala en las redes de grupo de trabajo, departamentales o aun de campus (o que ni siquiera llegaron a serlo) ahora pasan a ser prioritarios. Esto se puede ilustrar mediante una tarea simple, como el soporte de la información acerca de las cuentas de usuario.

La forma más simple de resolver dicho problema es almacenar los datos de las cuentas de todos los usuarios en una base de datos local de cuentas de usuarios en cada computadora. Cuando un usuario intente tener acceso a estos recursos, los datos requeridos son recuperados de la base de datos local de cuentas de usuarios. Con base en esta información, el acceso puede otorgarse o negarse. Este método funciona bien en pequeñas redes de cinco a 10 computadoras; sin embargo, si la red tiene varios miles de usuarios, cada uno de los cuales necesita acceder a decenas de servidores, esta solución será algo extremadamente ineficaz. Los administradores deben repetir la operación de crear cuentas de usuario tantas veces como servidores haya en la red; además, el usuario final está obligado a repetir el procedimiento de acceso cada vez que sea necesario el acceso a los recursos de un nuevo servidor. Una buena solución a este problema en una red corporativa consiste en emplear un servicio de

directorio centralizado, cuya base de datos pueda almacenar cuentas de todos los usuarios de la red. El administrador realiza la operación de crear cuentas de usuario solamente una vez, y el usuario tiene que ingresar a la red solamente una vez (observe que en este caso el usuario ingresa a toda la red, en lugar de hacerlo a un solo servidor).

Cuando se migra de redes sencillas a redes más complejas, de redes departamentales a ambientes corporativos, las distancias geográficas se hacen más grandes y soportar las comunicaciones entre computadoras se convierte en una tarea cada vez más compleja y costosa. A medida que el tamaño de la red crece, los requerimientos de confiabilidad, desempeño y funcionalidad aumentan en la misma proporción. Los volúmenes de datos que circulan a través de una red se hacen mayores y, además de la disponibilidad de dichos datos, la red debe encargarse de su seguridad. Todos estos factores resultan en la construcción de redes corporativas basadas en equipo y software más poderoso y versátil.

5.5 INTERNET

PALABRAS CLAVE: Internet, pila de protocolos TCP/IP, servicio de hipertexto WWW, proveedor de servicios de Internet (ISP), unicidad de Internet, contenido, correo electrónico, FTP, VPN grado 1, grado 3, grado 4, ISP de troncal, ISP regionales, ISP locales, central de Internet (IX), punto de acceso a la red (NAP), proveedor de servicios de cobro, proveedores de servicios de aplicación, proveedores de distribución de contendido y proveedor de hospedaje.

Internet no sólo es una red, sino también un fenómeno de la civilización actual. Los cambios que dieron como resultado la llegada de Internet son multifacéticos. El servicio de hipertexto WWW ha cambiado de manera radical el método de presentar información mediante la combinación de texto, gráficas y sonido dentro de las páginas web. El transporte de Internet —barato y disponible en prácticamente todas las compañías y para todas las personas a través de las redes telefónicas— ha simplificado en gran medida la tarea de construir redes corporativas. Al mismo tiempo, ha traído a un primer plano la importante tarea de proteger los datos de las redes corporativas durante su transmisión mediante el uso de redes públicas que soportan a millones de usuarios. La pila de protocolos TCP/IP, en la cual se basa la red Internet en su totalidad, se ha convertido en la pila de protocolos más popular.

Internet evolucionó de manera continua para convertirse en la red mundial de las comunicaciones públicas. Su uso ha aumentado en forma gradual tanto para la publicación de información (incluidas promociones) como para realizar transacciones de negocios, por ejemplo: la compra de bienes y servicios y la transferencia de activos financieros. Para muchas compañías, lo anterior significa un cambio radical en la forma de hacer negocios; además, esto modifica el comportamiento de los clientes, ya que más personas empiezan a inclinarse por las operaciones de negocios de forma electrónica.

5.5.1 Unicidad de Internet

La característica de Internet de ser *única* se manifiesta de varias formas:

- Es la red *más grande* del mundo en cuanto a número de usuarios, cobertura, cantidad de tráfico que genera y número de redes conectadas. Aunque la velocidad de crecimiento de Internet ha disminuido ligeramente desde la revolución de Internet a mediados de la década de 1990, aún se conserva elevada y ha excedido de manera significativa la velocidad de crecimiento de las redes telefónicas.

- Internet es una red que *no cuenta con un centro de control*; sin embargo, trabaja de acuerdo con reglas, proporcionando a todos sus usuarios un conjunto unificado de servicios. Internet es la red de redes, pero cualquier red conectada a ella es administrada por un operador independiente llamado **proveedor de servicios de Internet (ISP)**. Existen algunas autoridades centrales, aunque sólo son responsables de unificar la política técnica, de un conjunto coordinado de estándares técnicos y de asignar de manera centralizada parámetros muy importantes en una red de estas proporciones. Esto incluye los nombres y direcciones de computadoras y redes conectadas a Internet; sin embargo, éstas no son responsables del mantenimiento diario de Internet o de proporcionarle soporte en un estado útil.
- Este alto grado de descentralización tiene ventajas y desventajas. Una ventaja es la *facilidad de crecimiento*; por ejemplo, para comenzar un negocio, es suficiente que un nuevo ISP concluya un acuerdo con al menos uno de los ISP existentes, después de lo cual todos los usuarios del nuevo ISP pueden acceder a todos los recursos de Internet. Entre las consecuencias negativas de la descentralización se incluyen las complicaciones relacionadas con la modernización de las tecnologías y servicios de Internet. Los cambios radicales requieren esfuerzos coordinados de todos los ISP (observe que si la red tuviera un solo propietario, dichas modificaciones serían mucho más sencillas). Debido a estas complicaciones, muchas tecnologías nuevas muy prometedoras se utilizan solamente dentro de la red de un solo propietario. Un buen ejemplo es la tecnología de difusión de grupo (broadcasting), la cual es necesaria para la organización eficaz de la difusión de audio y video a través de Internet. Esta tecnología aún no puede superar las fronteras que separan a los ISP. Otro ejemplo es la relativamente baja confiabilidad de los servicios de Internet. Esto se debe a que ningún ISP es responsable del resultado final, por ejemplo: el acceso del cliente A al sitio B si ambos pertenecen a redes de ISP diferentes.
- Internet es una *red barata*; por ejemplo, la popularidad del nuevo servicio de Internet —telefonía por Internet— es, en muchos sentidos, el resultado de sus tarifas significativamente bajas para las comunicaciones telefónicas internacionales, comparadas con las tarifas de las redes telefónicas convencionales. Aún más importante es que estas bajas tarifas no son resultado de la reducción de precios temporal que se utiliza como truco de mercadotecnia de compañías que desean conquistar nuevos mercados. Por el contrario, las bajas tarifas son provocadas por razones objetivas, por ejemplo: el costo significativamente menor de las características de la infraestructura de transporte de Internet para las redes de conmutación de paquetes, en comparación con la infraestructura de las redes telefónicas tradicionales. Desde luego, existen algunas expectativas de que Internet se haga más cara con el tiempo a medida que las tecnologías y servicios sean más avanzados. Los diseñadores de las tecnologías de Internet y los ISP saben acerca de este riesgo y, por lo tanto, analizan cada innovación desde este punto de vista.

Sin embargo, Internet nunca se hubiera convertido en lo que es hoy si no tuviera otra característica única: su vasto **contenido** informativo y la *facilidad de acceso a dicho contenido* para todos sus usuarios. Internet almacena terabytes de información disponible a los usuarios finales como páginas web. Hasta 1991, Internet era una red popular para una audiencia de usuarios más o menos pequeña, pero a nivel mundial. Dichos usuarios eran principalmente empleados y estudiantes de universidades y centros de investigación. Los demás clientes, como grandes corporaciones, bancos y organizaciones gubernamentales que requerían servicios de redes de datos, utilizaban otras redes de paquetes, como la X.25.

Ni las redes X.25 ni las *Frame Relay* que las reemplazaron a mediados de la década de 1990 tenían algo parecido al servicio WWW. Con la llegada de la web, los usuarios compren-

dieron de inmediato que algo apropiado y útil había llegado. Antes de la invención de la web, Internet era utilizado principalmente como sistema de información, no como transporte. El correo electrónico y los archivos FTP ya existían desde los primeros años de la aparición de Internet; sin embargo, las herramientas que daban acceso a la información textual almacenada en los archivos FTP, que proporcionaban principalmente los resultados de la investigación científica, eran muy primitivas. En consecuencia, la búsqueda de la información por nombre de archivo requería horas o incluso días.

Algunas formas convenientes de presentar las interrelaciones entre las diferentes partes del contenido de la información, como los hiperenlaces y el navegador gráfico estándar —el cual corre de modo fácil y eficaz en todos los sistemas operativos—, dieron como resultado la revolución de Internet. Dicha red fue saturada de inmediato con información presentada como páginas web, que gradualmente se convirtieron en enciclopedias, periódicos, agencias de promoción y una gran tienda. En la actualidad, muchas personas no pueden imaginar su vida sin navegar en la web: para comunicarse con amigos, para buscar información urgente, para conseguir un nuevo trabajo o para pagar las cuentas.

NOTA *Sin embargo, sería incorrecto pensar que la tecnología de Internet ha obligado o esté obligando a las demás tecnologías de red a caer en el desuso. Esto se halla muy lejos de ser verdad y no es muy probable que suceda. La TCP/IP es la tecnología de interconectividad de redes que deja espacio a otras tecnologías, es decir, las que se utilizan en cada red independiente que conforma Internet. Por lo tanto, el éxito de Internet no constituye una razón para estudiar solamente las tecnologías TCP/IP. En las redes modernas, el protocolo TCP/IP de forma muy cercana con muchas otras tecnologías, como Ethernet, ATM, Frame Relay, MPLS y ADSL.*

5.5.2 Estructura de Internet

El rápido crecimiento en el número de gente que es atraída por el contenido informativo de los sitios web ha cambiado de manera significativa la actitud de los usuarios corporativos y los proveedores de servicios de telecomunicaciones hacia esta red. En la actualidad, prácticamente todos los prestadores de servicios de telecomunicaciones convencionales soportan Internet; además, muchas nuevas compañías han creado negocios exclusivamente con base en el ofrecimiento de servicios de Internet. Por lo tanto, la estructura general de Internet que se muestra en la figura 5.7 es, en muchos sentidos, un reflejo de la estructura general de la red mundial de telecomunicaciones, un fragmento de la cual se mostró en la figura 5.3.

Existen varias formas de clasificar los ISP. La figura 5.7 muestra una de ellas, la cual es similar a la clasificación existente de los proveedores de servicios de telecomunicaciones. De acuerdo con esta clasificación, las características principales de un ISP son su cobertura, territorio y el conjunto de servicios que brinda. Los **ISP de troncal** son similares a los proveedores de servicios internacionales de telecomunicaciones, quienes son propietarios de troncales que cubren territorios muy vastos (países específicos, continentes o todo el mundo). Ejemplos de ISP troncales son compañías como Cable & Wireless, MCI y Global One. De acuerdo con esto, los **ISP regionales** proporcionan servicios de Internet dentro de los límites de regiones específicas (estado, condado y distrito, lo cual depende de la división administrativa adoptada por los diferentes países) y los **ISP locales** generalmente prestan servicios de Internet dentro de los límites de una ciudad.

Las relaciones entre los ISP están basadas en *acuerdos comerciales de igual a igual* para la mutua transmisión del tráfico. Los proveedores de troncales por lo general tienen dichos acuerdos con los demás proveedores de troncales (ya que éstos no son muy numerosos), y los

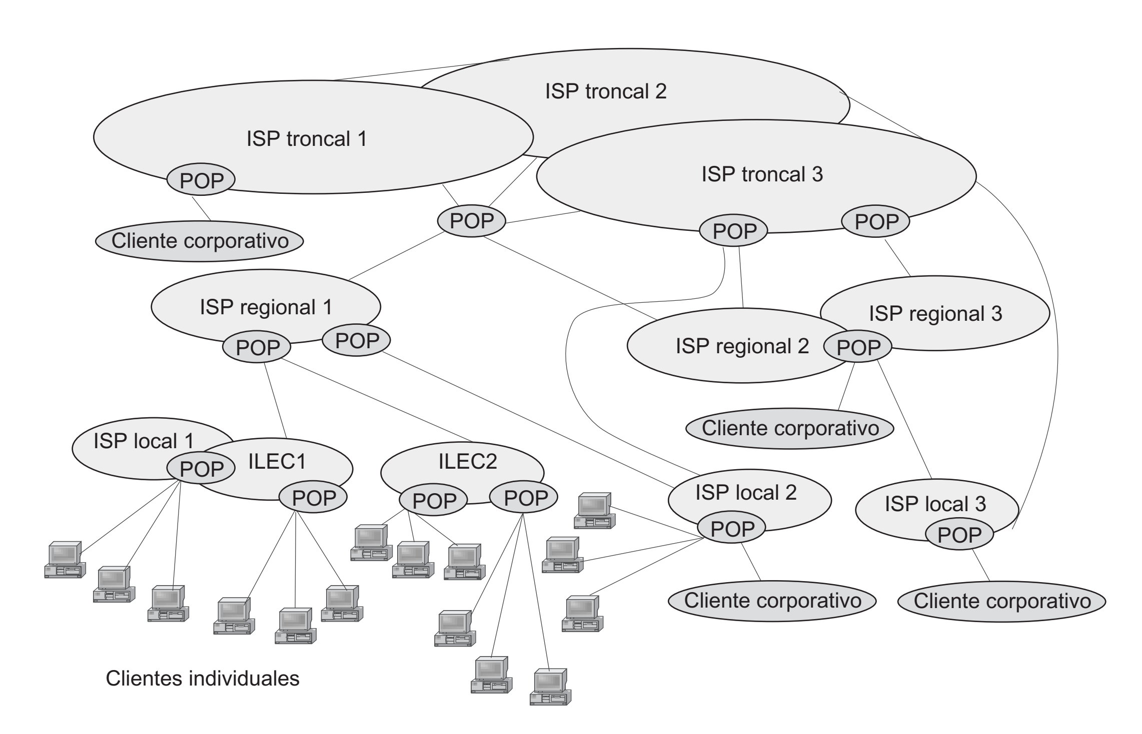


FIGURA 5.7 Estructura de Internet.

proveedores regionales suelen hacer tratos con uno de los proveedores de troncales y algunos otros proveedores regionales. Al mismo tiempo, los proveedores configuran sus equipos con el fin de asegurarse de que el tráfico circula de una red a otras en ambas direcciones.

PUNTOS DE ACCESO A LA RED/CENTRAL DE INTERNET

Para simplificar el proceso de organizar las comunicaciones entre los proveedores regionales, existen centros especiales de intercambio en Internet, a los cuales se encuentran conectadas las redes de muchos proveedores. Dichos centros de intercambio pueden ser soportados por proveedores específicos de alto nivel (nacionales o internacionales) para proveedores de bajo nivel conectados a la red. Los centros de intercambio pueden ser soportados por compañías dedicadas a llevar a cabo esta tarea. Dichos centros de intercambio tienen nombres diferentes: por lo general centrales de internet (IX) o puntos de acceso a la red (NAP).

El papel que desempeña el NAP/IX en el intercambio de tráfico entre redes de ISP puede variar. En el caso de una variación mínima, dicho centro simplemente proporciona a los ISP las facilidades para instalar el equipo de comunicaciones. Los ISP establecen todas sus conexiones físicas y lógicas. La situación en la que el equipo de telecomunicaciones del NAP/IX forma parte en el intercambio de tráfico entre los ISP, es más común. En este caso, el NAP/IX solamente proporciona conexiones físicas entre el equipo de todos los ISP, sin crear conexiones lógicas entre las redes ISP para el intercambio de tráfico. Por lo tanto, los ISP conectados al NAP/IX utilizando este método todavía tienen que efectuar cambios entre sí. Por último, existen centros de intercambio de datos que combinan las funciones de intercambio de datos con funciones comerciales. Estos centros, conocidos como centros coordinadores, trabajan como casas de bolsa para comercializar anchos de banda. Todos los ISP conectados a dichos centros declaran sus costos de transmisión de datos y el centro desempeña el papel de moderador en el momento en que se efectúan los arreglos.

Otra clasificación popular de ISP los divide en cuatro categorías: **grado 1**, **grado 2**, **grado 3** y **grado 4** (consulte la página http://www.nwfusion.com).

Las definiciones de los ISP grado 1, grado 3 y grado 4 coinciden con las definiciones proporcionadas con anterioridad de los *ISP* troncales, regionales y locales. Sin embargo, la categoría grado 2 se define para tipos especiales de *ISP*.

Un ISP grado 2 proporciona servicios de Internet a un gran número de usuarios finales en un país en particular o aun más, en todo un continente; asimismo, brinda una amplia gama de servicios de información y comunicaciones. Estos ISP son similares a un ISP local en el sentido que trabajan directamente con los usuarios de Internet; sin embargo, la escala del área de cobertura los distingue de los proveedores locales. Compañías como America Online son *ISP* grado 2.

La llegada de los ISP grado 2 está basada en los arreglos con muchos prestadores de servicios de telecomunicaciones locales que no proporcionan servicios de Internet por sí mismos. En la figura 5.7, la compañía ILEC2 es un ejemplo de dicho prestador de servicios y cuenta con loops locales inicialmente diseñados para tráfico telefónico. En la actualidad, sus suscriptores pueden utilizar los mismos canales físicos para transmitir datos mediante el uso de módems. En la actualidad se aplican dos tipos de módems en los loops locales: conmutados y la línea de suscriptor digital asimétrica (ADSL). Los módem conmutados conectan la computadora de los usuarios terminales a la red ISP de manera temporal, de forma semejante a como el teléfono conecta al usuario a la red telefónica sólo por el tiempo que dura la conversación. Un módem ADSL asegura una conexión persistente entre una computadora y una red ISP.

Como el ILEC2 proporciona solamente servicios de telefonía, éste separa el tráfico telefónico del tráfico de datos en su POP. Después procesa el tráfico telefónico de la manera usual, utilizando switches telefónicos y enviando el tráfico de datos al ISP con el que ha hecho acuerdos (el ISP1 regional en la figura 5.7). Si el ISP tiene acuerdos con un mayor número de operadores locales se convierte en un ISP grado 2, que no cuenta con infraestructura propia para el acceso de los clientes.

Como regla, los ISP grado 2 interactúan con otros ISP a través de un ISP grado 1, el cual transmite su tráfico de larga distancia y brinda otros servicios de gran utilidad, como el establecimiento de pagos mutuos.

La interpretación descrita previamente de los términos grado 1 hasta grado 4 no es la única que existe; por ejemplo, en algunos libros puede encontrar que las definiciones de estos términos tienen en cuenta sólo el territorio cubierto por los servicios (es decir, éstos coinciden con las definiciones de ISP internacionales, troncales, regionales y locales).

También es posible clasificar los ISP de acuerdo con los tipos de servicios que brindan. En este caso, el término genérico *ISP* se aplica generalmente a compañías que sólo brindan servicios de transporte a los usuarios finales; esto es, aseguran la transmisión de su tráfico hacia las redes de otros ISP.

- Si un ISP tiene sus sitios web y los llena de contenido, éste se conoce como **proveedor de contenido de internet (ICP)**. La mayoría de los ISP son también ICP debido a que soportan sus propios sitios de información.
- Si la compañía proporciona las instalaciones, enlaces y servidores para almacenar el contenido generado por otras compañías, se llama **proveedor de hospedaje**.
- Existen también los **proveedores de distribución de contenido (CDPS)**, los cuales no crean contenido pero están involucrados en el hospedaje de contenido en múltiples lugares cercanos a los del usuario, con el fin de incrementar la velocidad de acceso a su información.

- Los **proveedores de servicios de aplicación (ASP)** proporcionan a los clientes acceso a productos de software universales de gran escala que son de soporte difícil. En general, se trata de usuarios corporativos interesados en las aplicaciones para la administración de la compañía, como SAP R3.
- Puesto que Internet se convirtió en un fenómeno de la vida social, el número de proveedores que ofrecen servicios sigue creciendo. Por ejemplo, algunas compañías ofrecen un servicio para el pago universal de cuentas **(proveedor de servicios de pagos**) en cooperación con las autoridades municipales y los proveedores de aire acondicionado y electricidad.

5.5.3 Fronteras de Internet

Ahora, examine las fronteras de Internet. Después de leer esta sección, usted probablemente se haga una pregunta razonable: ¿será posible establecer las fronteras de Internet si ésta se encuentra integrada a la infraestructura de los prestadores de servicios de telecomunicaciones?

Para contestar dicha pregunta, considere con más detalle una red típica de un ISP y su cliente (figura 5.8).

El ISP que se considera en este ejemplo cuenta con dos clientes corporativos y un gran número de clientes individuales. Naturalmente, este ISP también cuenta con varias conexiones a otros ISP a través de los cuales obtiene acceso a los demás ISP que conforman Internet. En la red Internet hay varios servidores que hospedan sitios web, los cuales están disponibles para todos los usuarios de Internet; sin embargo, el cliente CC1 también tiene recursos informativos que contienen información confidencial de la compañía.

Dichos recursos deben estar disponibles solamente para los empleados de la corporación. Por lo tanto, el cliente corporativo CC1 tiene instalados dispositivos de comunicaciones especializados en sus redes, conocidos como firewalls (cortafuegos). Un firewall protege la parte de la red que contiene servidores diseñados para uso interno, con los cuales permite que sólo los clientes localizados dentro de esa red tengan acceso a dichos servidores. Todas

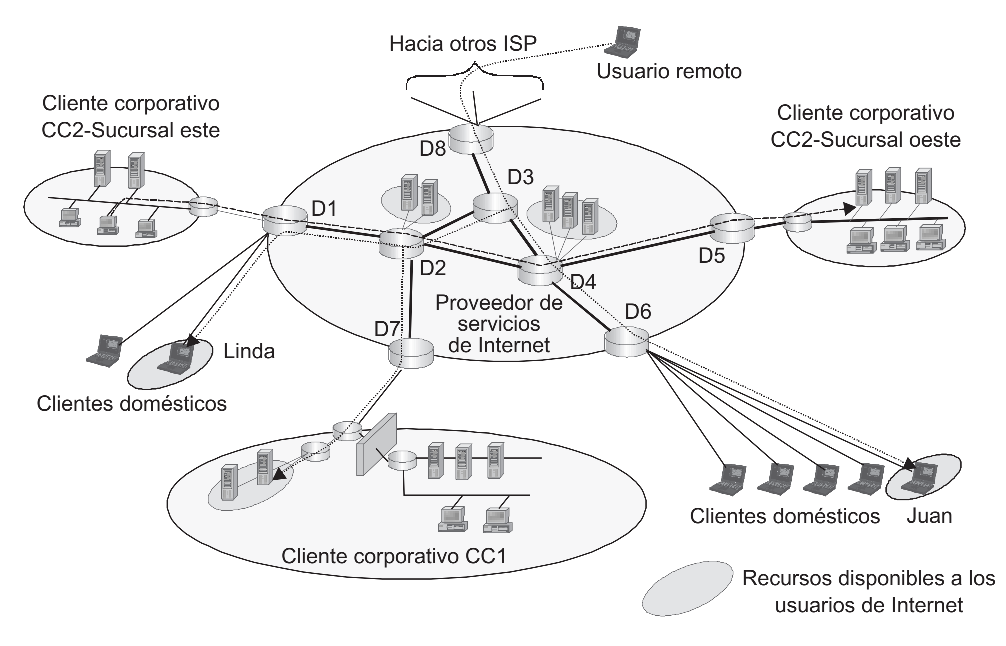


FIGURA 5.8 Fronteras de Internet.

las solicitudes de acceso a estos servidores por parte de clientes externos son bloqueadas por el firewall. Un firewall permite el acceso de los clientes internos a recursos de información externos (es decir, recursos de Internet). También transfiere las respuestas de los servidores externos a los empleados corporativos. Si los usuarios corporativos no necesitan acceso a los recursos de Internet, sería más fácil desconectar físicamente la red interna desde la red ISP, en vez de instalar un firewall.

El cliente corporativo CC1 tiene su red, la cual incluye varios servidores que almacenan información y numerosas computadoras utilizadas por los empleados de la compañía. Este cliente cuenta con una conexión de alta velocidad al ISP y utiliza el servicio básico de acceso a Internet que asegura el intercambio de datos entre la red corporativa y la red ISP. Las redes ISP también operan como redes de tránsito para el intercambio de datos con las redes de otros ISP. El cliente CC1 soporta varios sitios web por sí mismo, los cuales están disponibles para todos los usuarios de Internet.

La mayoría de los clientes individuales del ISP de la figura 5.8 se conectan a su red mediante el uso de módems conmutados. Dos clientes individuales —Juan y Linda— tienen conexiones persistentes a la red ISP mediante módems ADSL. Juan y Linda han creado sitios web personales en sus computadoras en casa y cada usuario de Internet puede conectarse con ellos y utilizar la información contenida en sus sitios.

El cliente corporativo CC2 tiene dos divisiones ubicadas en diferentes ciudades: la sucursal oeste y la este. Cada una de estas divisiones cuenta con su propia LAN. Estas redes se basan en la tecnología TCP/IP, la cual se utiliza en Internet. El cliente CC2 usa el ISP para conectar las redes de la división a la red corporativa en lugar de adquirir el acceso a Internet, porque este cliente no lo necesita. Por el contrario, esta compañía debe asegurar un alto nivel en la seguridad de sus datos. Debido a esto y en contraste con el cliente CC1, la compañía CC2 utiliza el servicio VPN proporcionado por su ISP en lugar de proteger sus recursos por sí mismo. El servicio VPN asegura que las dos redes de los clientes CC2 estarán aisladas del tráfico de Internet. Por lo tanto, todos los recursos de información de estas dos redes —sitios web, bases de datos, etc.— estarán a disposición sólo de los usuarios internos. Los empleados de la compañía CC2 no pueden utilizar los servicios que brinda Internet, ya que sus solicitudes no se envían hacia Internet.

Ahora conteste nuestra pregunta, ¿es la red ISP parte de Internet? Por un lado, usted puede contestar que sí, ya que ésta transmite tráfico del cliente hacia Internet y contiene recursos de información públicos. El usuario remoto de Internet que se muestra en la figura 5.8 puede solicitar acceso a cualquier sitio web del ISP.

Por otro lado, parte de la infraestructura de transporte del ISP no está relacionada con Internet. La lista de dichos dispositivos de red incluye los dispositivos de comunicaciones D5 utilizados exclusivamente para soportar la operación del cliente CC2 y el enlace que conecta D5 con D4. Además, la red ISP contiene dispositivos y enlaces que sirven sólo en forma parcial a los clientes de Internet: los dispositivos D1, D2 y D4, así como los enlaces que conectan a dichos dispositivos.

Debido a lo anterior, la respuesta *sí* no refleja la situación en forma precisa. Las fronteras de la red ISP no coinciden con las de Internet, a pesar de esta última red está formado por redes ISP.

Una situación similar se presenta en la red del cliente CC1. Por otro lado, es posible decir que la red no es parte de Internet debido a que esta compañía no es un ISP; más bien, es un cliente. Además, la red CC1 contiene recursos protegidos por un firewall, los cuales, en consecuencia, no son parte de Internet. Por otro lado, la red CC1 contiene sitios web disponibles a todos los usuarios de Internet, incluido el usuario remoto. Desde el punto de vista del cliente remoto, estos sitios web no son diferentes de los sitios web localizados dentro de la

red ISP. La red CC1 también contiene recursos protegidos por un firewall. Como es natural, los recursos protegidos mediante un firewall no son parte de Internet.

Los clientes domésticos que se conectan a Internet mediante conexiones conmutadas suelen no instalar sus sitios web en sus computadoras caseras, debido a que estos sitios podrían no estar disponibles a otros usuarios de Internet la mayor parte del tiempo. Sin embargo, los usuarios domésticos que cuentan con conexiones permanentes a Internet a través de módems ADSL pueden hacerlo. En la red de la figura 5.8, Juan y Linda dan soporte a sus sitios web y los usuarios remotos pueden utilizar su contenido cuando así lo deseen.

Desde el punto de vista de sus usuarios, Internet proporciona un conjunto de recursos de información distribuidos en redes diferentes: redes ISP, redes corporativas, redes caseras y las computadoras de los usuarios individuales.

Las herramientas de transporte de Internet también son virtuales. Es posible considerarlas parte de los recursos (dispositivos y enlaces de comunicaciones) de los prestadores de servicios de telecomunicaciones que aseguran la transmisión de tráfico de Internet: esto es, el tráfico entre los clientes de Internet y los recursos de información (o entre dos clientes de Internet, en el caso de tráfico de correo electrónico o de tráfico telefónico por Internet).

En general, la red de un ISP se denomina *red IP privada*, debido a que con el uso de esta red, el prestador de servicios generalmente proporciona tanto servicios de Internet como otro tipo de servicios, tales como VPN. Si lo anterior se lleva a cabo utilizando las tecnologías en las que se basa Internet (es decir, el transporte TCP/IP y el servicio de información WWW), dichos servicios se llamarán **servicios intranet**.

RESUMEN

- Las redes de computadoras proporcionan servicios de dos tipos: de información y de transporte. Con mucha frecuencia, el término *servicios de red* se interpreta como servicios de transporte, lo cual considera que la transmisión de información representa el papel principal de la red. Los servicios de información son ofrecidos por los nodos terminales de la red (los servidores), mientras que los servicios de transporte son proporcionados por los nodos de tránsito (los switches y ruteadores de la red).
- Las redes de computadoras pueden describirse mediante una estructura generalizada aplicable a cualquier red de telecomunicaciones. Dicha estructura incluye los componentes que siguen: *red de acceso, troncal* y *centros de datos*.
- Los *proveedores de servicios de telecomunicaciones* son compañías especializadas que construyen redes de telecomunicaciones con el fin de brindar servicios públicos; son propietarios de estas redes y dan el soporte para su operación.
- Los proveedores de servicios de telecomunicaciones difieren entre sí por el conjunto de servicios que prestan, el territorio dentro del cual se proporcionan estos servicios, el tipo de clientes para los que los diseñaron y la infraestructura con la que cuenta dicho prestador de servicios. En esta última se incluyen enlaces, equipo de comunicaciones y servidores de información. Los proveedores de servicios de telecomunicaciones que se especializan en brindar servicios a las redes de computadoras se conocen comúnmente con el nombre de *proveedores de servicios*.
- Una red corporativa es aquella cuyo objetivo principal consiste en proporcionar soporte a la operación de la compañía propietaria de dicha red. Los usuarios de una red corporativa son los empleados de la compañía.
- Internet es una red de computadoras única que proporciona varios servicios en todo el mundo. Internet utiliza la pila de protocolos TCP/IP para interconectar redes basadas

en varias tecnologías. Como resultado de la popularidad de Internet y sus servicios de información (correo electrónico, web y chat), los protocolos de transporte de la pila TCP/IP se usan para construir interredes.

PREGUNTAS DE REPASO

1. ¿Qué término corresponde a la definición siguiente: "Red diseñada para concentrar flujos de información que llegan a través de enlaces múltiples desde el equipo de los usuarios finales?
   a) Troncal
   b) Red de acceso
   c) Red principal
   d) Red operativa
2. Proporcione ejemplos de centros de datos de diferentes tipos de redes de telecomunicaciones.
3. Haga una lista de los requerimientos principales de las redes de acceso y redes troncales.
4. Haga una lista de los tipos de clientes que pueden tener los proveedores de servicios de comunicaciones.
5. ¿Cuándo se puede llamar *red corporativa* a una red proveedora de servicios?
6. ¿Cuáles son las características principales de las redes proveedoras de servicios de comunicaciones?
7. ¿Son convencionales los servicios de líneas arrendadas o constituyen un nuevo desarrollo de los proveedores de servicios de telecomunicaciones?
8. ¿Qué servicios adicionales brinda un proveedor competitivo que apenas comienza su negocio con el fin de atraer clientes?
9. ¿Cuál es la diferencia entre los ISP grado 1 y grado 2?
10. ¿Qué tipo de servicio brinda el acceso a Internet?
11. ¿Es posible que un proveedor de servicios de telecomunicaciones brinde acceso a Internet sin que sea propietario de enlaces de comunicaciones?
12. Establezca la correlación entre las descripciones de las redes y sus tipos (un tipo de red no se describe).

Tipo de red	Red corporativa	Red de campus	Red departamental	Red de proveedor de servicios de telecomunicaciones
Utilizada por un grupo de empleados (100-150 usuarios). Todos los usuarios de la red resuelven una tarea en particular del negocio. Se basa en una sola tecnología.				

Continúa

Continuación

Tipo de red	Red corporativa	Red de campus	Red departamental	Red de proveedor de servicios de telecomunicaciones
Miles de computadoras y cientos de servidores. Alto nivel de heterogeneidad de las computadoras, equipo de comunicaciones, sistemas operativos y aplicaciones. Se utilizan enlaces WAN.				
Conectan redes más pequeñas dentro de los límites de un edificio No se usan enlaces WAN. Los servicios proporcionan acceso a todos los empleados a las bases de datos de la compañía.				

13. ¿En qué tipo de redes (corporativas o ISP) tienen mayor participación las LAN?
14. ¿Cuáles son los niveles jerárquicos en los que se puede dividir una red corporativa?
15. Haga una lista de los tipos de especializaciones ISP.
16. Si una red corporativa tiene una conexión permanente a Internet, ¿esto significa que dicha red es parte de Internet?

PROBLEMAS

1. ¿Cómo puede un proveedor de servicios local competitivo proporcionar acceso a clientes individuales a los recursos de su red?
2. ¿Qué problemas tuvieron que resolverse para eliminar los monopolios en la industria de las telecomunicaciones?
3. Describa el servicio de red privada virtual para los suscriptores telefónicos.
4. Describa la secuencia de pasos que la administración de la compañía debe realizar para convertirla en un ISP y comenzar a brindar servicio a sus clientes.
5. Un ISP es propietario de una troncal y de redes de acceso. ¿A qué tipo de red conviene conectar un nuevo centro de datos?

6

CARACTERÍSTICAS DE LAS REDES

DESCRIPCIÓN DEL CAPÍTULO

6.1 INTRODUCCIÓN

Las redes de computadoras son sistemas complejos y costosos que llevan a cabo tareas críticas y que brindan servicios a un gran número de usuarios. Por ello, es importante asegurar no solamente la operación de la red, sino también la confiabilidad y la alta calidad de dicha operación.

El concepto de *calidad de servicio* puede interpretarse en un sentido amplio y puede incluir todas las propiedades factibles de la red y del proveedor del servicio que son deseables para el usuario final. Para permitir que tanto el usuario como el proveedor de servicios estudien los problemas del servicio y establezcan relaciones de manera formal, existen varias características comúnmente adoptadas en una red. En este capítulo estudiaremos las características relacionadas con la calidad de los servicios de transporte de la red, las cuales son más fáciles de formalizar que las características relacionadas con la calidad de los servicios de información. Las características de transporte reflejan propiedades importantes de la red, como el desempeño, la confiabilidad y la seguridad.

Algunas de estas características pueden evaluarse de modo cuantitativo y medirse en el momento en que se brinda el servicio a los usuarios. El usuario y el prestador de servicios pueden elaborar el famoso *Acuerdo sobre el nivel del servicio*, especificando los requerimientos de los valores cuantitativos de algunas características, como la disponibilidad del servicio.

El concepto de calidad de servicio se utiliza a veces en un sentido restringido, como un concepto de tendencias modernas de las tecnologías de las redes y, en este caso, se utilizan las siglas QoS. Esta tendencia se halla dirigida al desarrollo de métodos que aseguren la transmisión de alta calidad del tráfico que usa la red. Las características de QoS tienen algo en común: todas reflejan el efecto negativo del mecanismo de colas sobre la transmisión de tráfico, como la disminución temporal de la velocidad de entrega de tráfico, retardos variables en la entrega de paquetes y la pérdida de paquetes debida a la saturación de las memorias de los switches. Los métodos para asegurar la QoS se estudiarán en el capítulo siguiente.

6.2 TIPOS DE CARACTERÍSTICAS

PALABRAS CLAVE: tráfico, calidad del servicio QoS, desempeño, confiabilidad, seguridad, características del proveedor único, mecanismo de colas, requerimientos, características a largo plazo, características a mediano plazo, características a corto plazo, control de la congestión, supresión de la congestión, *Acuerdo sobre el nivel del servicio* (SLA).

6.2.1 Características subjetivas de calidad

Si se efectúa un sondeo entre varios usuarios con el fin de clarificar lo que quieren decir cuando hablan acerca de la calidad de los servicios de conectividad, se obtendrá una gran gama de respuestas, entre las cuales pueden estar las siguientes:

- La red trabaja de manera rápida y sin retardos.
- El tráfico se transmite de modo confiable.
- El servicio se brinda de forma continua.
- Los servicios de soporte y de ayuda trabajan bien, ofrecen consejos útiles y ayudan a resolver problemas.

- El servicio se ofrece de acuerdo con un plan flexible. Quisiera que la velocidad de acceso a la red pudiera ser mucho más rápido en todo momento.
- El proveedor de servicios no sólo transmite el tráfico que genero, sino también protege mi red contra ataques de virus e intrusiones.
- Siempre puedo verificar qué tan rápido mi proveedor transmite mi tráfico y si se presentan pérdidas en mis datos.
- Además del acceso estándar a Internet, el proveedor ofrece una amplia gama de servicios complementarios, como el hospedaje de mi sitio web personal y los servicios de telefonía IP.

Estas evaluaciones subjetivas reflejan los deseos de los usuarios en relación con la calidad de los servicios de la red. Los clientes (usuarios) representan la parte más importante de cualquier negocio, incluidas las redes de datos; sin embargo, existe otra parte: el proveedor del servicio (comercial si la red es pública y no comercial si ésta es corporativa). Para hacer posible que tanto usuarios como proveedores de servicios evalúen objetivamente la calidad de los servicios de red, existen *características formalizadas de la calidad de los servicios de la red*, que permiten evaluar cuantitativamente aspectos específicos acerca de la calidad.

6.2.2 Características y requerimientos de las redes

Mediante el uso de las **características** de la red, el suscriptor puede formular **requerimientos** específicos de la red. Por ejemplo, el usuario puede exigir el requerimiento siguiente: *la velocidad promedio de transmisión de mi información a través de la red no debe ser menor que 2 Mbps.* En este caso, el usuario aplica la característica conocida como velocidad promedio de la transmisión de datos a través de la red, y define que el intervalo de valores de esta característica corresponda a una buena calidad de servicio para el usuario (es decir, la operación eficaz de la red).

Todas las características del QoS para el transporte de servicios pueden clasificarse en alguno de los siguientes grupos:

- Desempeño.
- Confiabilidad.
- Seguridad.
- Solamente por el proveedor.

Los primeros tres grupos corresponden a las propiedades del servicio de transporte, las cuales son las más importantes para el usuario. La red debe transmitir información a una velocidad específica (*desempeño*), sin pérdidas o retardos en el servicio (*confiabilidad*), y asegurar la protección contra el acceso no autorizado o falsificación (*seguridad*).

Como es natural, los proveedores de servicios que buscan la satisfacción de los clientes ponen atención a todas las características que son importantes para los usuarios. Al mismo tiempo, está el rango de características de la red, las cuales son vitales para los proveedores del servicio; sin embargo, no tienen mayor importancia para los usuarios.

Las redes dan servicio a un gran número de usuarios y los proveedores de servicios deben organizar sus operaciones para satisfacer de manera simultánea las necesidades que aquéllos tienen. Como regla general, esto representa un problema difícil, ya que los principales recursos de la red —enlaces y switches/ruteadores— son compartidos por los flujos de información de los usuarios. Los proveedores deben encontrar un balance en la distribución de recursos

entre flujos concurrentes que satisfagan las necesidades de los usuarios. La solución a este problema incluye la planeación del uso de los recursos y su control cuando se transmita tráfico de usuario. Por lo tanto, el interés del proveedor es en las características que describen las propiedades de los recursos utilizados para dar servicio a los clientes de la red. Por ejemplo, el proveedor está interesado en el desempeño del switch, ya que debe evaluar el número de flujos que pueden pasar por éste. Por otro lado, los usuarios finales no están interesados en el desempeño de un switch específico, sino en el resultado final: si su flujo de información se proporciona con una alta calidad o no.

El cuarto grupo combina las características QoS que son de interés para el proveedor de servicios solamente. Uno de los ejemplos de dichas características es la escalabilidad de la red (es decir, la posibilidad de incrementar el número de usuarios sin tener que cambiar las tecnologías de la red).

6.2.3 Escala de tiempo

Antes de estudiar las características y métodos de aseguramiento del QoS, sería de gran utilidad conocer otra clasificación: la escala de tiempo en la que están definidas estas características y con cuáles métodos de QoS trabajan.

Las **características a largo plazo** se definen en periodos que varían desde varios meses a algunos años. Éstas pueden llamarse características proyecto-solución y los métodos adecuados para asegurarlas son los *de planeación y diseño de la red*. Este grupo incluye soluciones a proyectos como la elección de modelos y número de interruptores (switches) o la selección de la topología de la red y los anchos de banda de los enlaces de comunicaciones. Estos parámetros influyen directamente en las características del QoS. Algunas soluciones a proyectos pueden resultar exitosas y equilibradas, con lo que se asegura que la red nunca se congestionará. Otras soluciones pueden ser menos eficaces y dar como resultado cuellos de botella en el tráfico, ya que las pérdidas de paquetes y los retardos exceden los límites máximos.

Como es obvio, el reemplazo total del equipo de red y las actualizaciones a gran escala de la red representan operaciones de trabajo muy intensas, que por lo general requieren un gasto significativo. Por lo tanto, dichas actualizaciones no se presentan con mucha frecuencia e influyen en el QoS a largo plazo.

Las **características a mediano plazo** están definidas mediante espacios de tiempo que van de varios segundos a algunos días. Ejemplos de dichas características son las velocidades promedio del flujo de tráfico o los retardos promedio en la entrega de paquetes, que se definen por espacios de tiempo muy grandes, durante los cuales se procesa un gran número de paquetes. Los métodos para determinar las rutas de tráfico representan un ejemplo de algunos métodos que trabajan en este rango; a su vez, las rutas de tráfico pueden permanecer inalteradas por horas o días, siempre que esa topología de red y los parámetros de tráfico permanezcan sin alteración y no fallen ni los enlaces de datos ni los switches de la red.

Las **características a corto plazo** están definidas mediante intervalos que corresponden a la velocidad de procesamiento de los paquetes individuales (es decir, en milisegundos o microsegundos). Este grupo incluye características como el tiempo de almacenamiento o el tiempo que debe esperar un paquete en la cola de un switch o de un ruteador. Los métodos diseñados específicamente para analizar y asegurar las características de este grupo se conocen como métodos para **controlar la congestión** y para **eliminar la congestión**, los cuales se describirán más a fondo.

6.2.4 Acuerdo sobre el nivel de servicio

El contrato o acuerdo constituye la base para la cooperación normal entre los proveedores de servicio y sus clientes (los usuarios finales). Los proveedores de servicios de las redes públicas de datos y sus clientes siempre realizan algún tipo de acuerdo; sin embargo, dichos acuerdos no siempre especifican los requerimientos cuantitativos respecto a la eficacia de los servicios brindados. Con mucha frecuencia, dicho acuerdo especifica el servicio que se proporcionará de manera muy general (por ejemplo, el acceso a Internet). Existe otro tipo de acuerdo, generalmente llamado **Acuerdo sobre el nivel de servicio** (**SLA**), en el cual el proveedor de servicios y el cliente describen la calidad de los servicios que se proporcionarán en términos cuantitativos mediante el uso de características comunes relacionadas con la eficacia de la red.

Por ejemplo, el SLA puede establecer que el proveedor está obligado a transmitir el tráfico del cliente sin pérdidas a la misma velocidad promedio a la que el cliente la envía a la red. El SLA también puede establecer que el presente acuerdo permanecerá vigente siempre y cuando la velocidad promedio del tráfico del cliente no exceda un valor específico (por ejemplo, 3 Mbps). De otra forma, el proveedor tiene el derecho a eliminar el tráfico en exceso. Para hacer dichos acuerdos más claros y para permitir que cada instancia controle su observancia, es necesario especificar el tiempo en el cual se medirá la velocidad promedio del tráfico (día, hora o segundo). El SLA es todavía más claro cuando se especifican tanto las herramientas como los métodos utilizados en la medición de las características de la red, de tal forma que el proveedor de servicios y el cliente comprendan el acuerdo sin ambigüedades.

Los SLA no solamente pueden realizarse entre proveedores de servicios comerciales y sus clientes, sino también dentro de grandes compañías. En este último caso, el SLA puede llevarse a cabo entre diferentes departamentos de la misma empresa (por ejemplo, el departamento de IT o departamento de telecomunicaciones) y el proveedor de servicios de red y entre los usuarios y los departamentos funcionales de la compañía, como es el departamento de producción.

6.3 DESEMPEÑO

PALABRAS CLAVE: velocidad de la información, retardo de paquetes, destrucción, histograma de distribución, densidad de la distribución del retardo de paquetes, métodos estadísticos, retardo promedio, variación de la fase, coeficiente de variación, retardo máximo, variación del retardo máximo, tiempo de respuesta de la red, tiempo del viaje redondo, velocidad de la información, velocidad constante de la información, velocidad comprometida de la información, velocidad pico de la información, tamaño de la ráfaga, coeficiente del tráfico en ráfagas, cantidad de ráfagas y cuellos de botella.

Usted ya conoce las características principales de los dispositivos de red: ancho de banda del enlace y desempeño de los dispositivos de telecomunicaciones, como los switches y los ruteadores. Éstas son características a largo plazo de recursos de la red que sólo son de interés para el proveedor de servicios. Si conocen dichas características, los proveedores podrán planear su negocio al determinar el número máximo de usuarios a los que pueden prestar el servicio.

Sin embargo, los usuarios están interesados en otras características del desempeño que les permitan llevar a cabo evaluaciones cuantitativas de la velocidad de tráfico y de la calidad de su transmisión. Para definir dichas características, se comenzará por considerar cómo transmite el tráfico una red ideal.

6.3.1 Redes ideales

Considere que la red será *ideal* si transmite cada bit de información con un retardo constante igual al retardo de la propagación de la luz en un medio físico; además, ningún enlace de red tiene un ancho de banda infinito: el ancho de banda del enlace es finito; por lo tanto, la fuente de información transmite paquetes hacia la red dentro de ciertos espacios de tiempo finitos en vez de hacerlo de forma instantánea. Este intervalo finito de tiempo, como usted sabe, es igual al cociente que se obtiene al dividir el tamaño de paquete (medido en bits) entre el ancho de banda del enlace.

La figura 6.1 muestra el resultado de transmitir paquetes a través de dicha red ideal. El eje superior muestra los tiempos de la transmisión de paquetes hacia la red desde el nodo de origen; el eje inferior muestra los tiempos de llegada de paquetes al nodo de destino. En otras palabras, el eje superior muestra la carga ofrecida de la red y en el inferior se muestran los resultados que se obtienen al transmitir este tráfico a través de la misma. Cuente los tiempos de llegada y salida de paquetes desde el instante de la transmisión del primer bit del paquete hacia la red y desde el instante de llegada del primer bit al nodo de destino, respectivamente.

Como se observa a partir de esta figura, la red ideal hace lo siguiente:

- Entrega todos los paquetes al nodo de destino, sin perder ni distorsionar ninguno de ellos.
- Entrega todos los paquetes en el mismo orden que fueron enviados.
- Entrega todos los paquetes con un retardo mínimo ($d_1 = d_2$, y así sucesivamente).

Es importante que todos los intervalos entre paquetes adyacentes permanezcan inalterados. Por ejemplo, el intervalo entre el primer paquete y el segundo era igual a τ_1 cuando se enviaron. Este valor permaneció igual cuando dichos paquetes llegaron al nodo de destino.

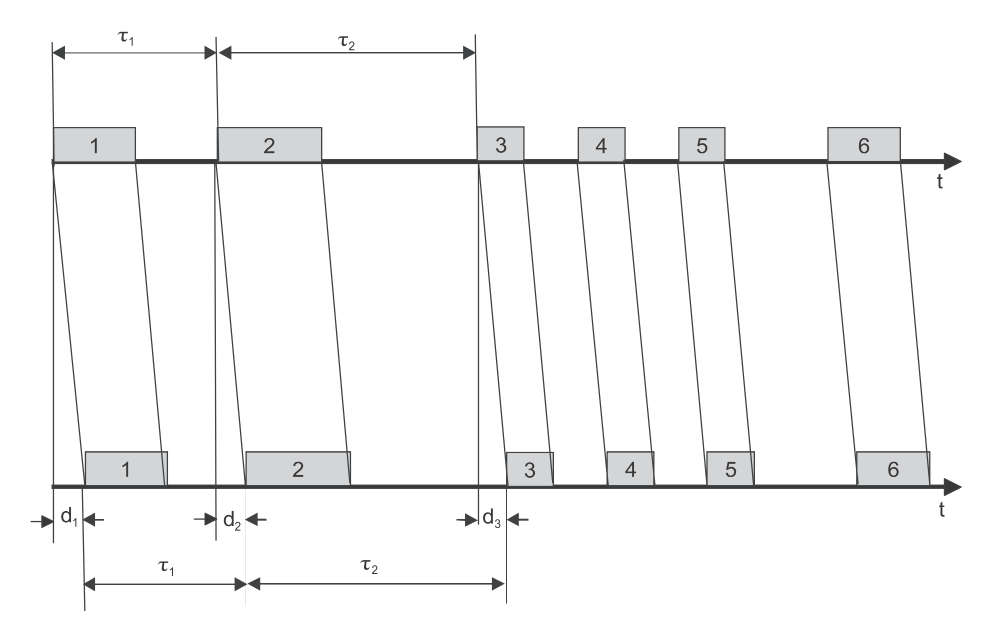


FIGURA 6.1 Transmisión de paquetes en una red ideal.

La entrega confiable de todos los paquetes con un mínimo de retardo y a un intervalo entre paquetes constante satisfará a todos los usuarios de la red sin importar qué tipo de tráfico se transmita a través de la misma: ya sea el de un servicio web o tráfico de telefonía IP.

Ahora se investigarán las desviaciones respecto al modelo ideal que podemos encontrar en una red real y las características que pueden utilizarse para describirlas (figura 6.2).

- Los paquetes son entregados al nodo de destino con *retardos variables*. Como usted sabe, ésta es una propiedad general de las redes de conmutación de paquetes. La naturaleza aleatoria del proceso de colas resulta en retardos variables; al mismo tiempo, los retardos en la entrega de algunos paquetes pueden ser considerables —decenas de veces mayores que el valor promedio de retardo ($d_1 \neq d_2 \neq d_3$, y así sucesivamente)—. Por lo tanto, la correlación en tiempo entre paquetes adyacentes varía, lo cual a su vez puede dar como consecuencia la aparición de fallas críticas en algunas aplicaciones. Por ejemplo, durante la transmisión digital de la voz, la variación en los intervalos entre paquetes da como resultado distorsiones significativas de la voz.
- Los paquetes pueden entregarse en el nodo de destino *en un orden diferente respecto al orden en que se enviaron*. Por ejemplo, el diagrama de la figura 6.2 muestra que el paquete 4 llegó al nodo de destino antes que el paquete 3. Estas situaciones pueden encontrarse en las redes de datagramas cuando se transmiten diferentes paquetes del mismo flujo a través de rutas distintas. En consecuencia, dichos paquetes esperan en cola con diversos niveles de retardo. Como es obvio, el paquete 3 circula a través de un nodo o varios nodos congestionados. Por lo tanto, su retardo total demostró ser tan grande que el paquete 4 llegó antes que él.
- *Los paquetes pueden perderse o dañarse*. Esta última situación es equivalente a la pérdida de paquetes, ya que la mayoría de los protocolos no puede recuperar los datos dañados. En la mayoría de los casos, los protocolos solamente pueden detectar que ocurrió un daño en los datos mediante el uso de la secuencia de verificación de las tramas (FCS).
- La velocidad promedio del flujo de información a la entrada del nodo de destino puede diferir de aquella con la que dicho flujo de información fue enviado hacia la red por el nodo de origen. Esto se debe a pérdidas de paquetes, más que a retardos de paquetes; por lo tanto, en el ejemplo que se muestra en la figura 6.2, *la velocidad promedio del flujo de salida disminuye* debido a la pérdida del paquete 5. A medida que más paquetes se pierden o se dañan, la velocidad del flujo de información es más baja.

Como es obvio, el conjunto de valores de los tiempos de transmisión de cada paquete individual definen una característica completa de la calidad de transmisión del tráfico; sin embargo, esta característica del desempeño de la red es muy extensa y redundante.

Para representar en forma compacta las características del QoS, es necesario utilizar **métodos estadísticos**. Las características estadísticas revelan dichas tendencias en el comportamiento de la red, las cuales parecen estables durante largo tiempo. Estas tendencias sólo pueden ser evidentes cuando se exploran las transmisiones de millones de paquetes. En las redes actuales, el tiempo de transmisión de un solo paquete está en el rango de microsegundos en la escala del tiempo. Por ejemplo, en Fast Ethernet, esta transmisión toma alrededor de 100 μs; en Gigabit Ethernet, alrededor de 10 μs; y en una celda ATM, desde fracciones de microsegundos hasta 3 μs (lo cual depende de la velocidad de transmisión). Por lo tanto, para obtener resultados estables, es necesario supervisar la red durante varios minutos o, aun mejor, durante varias horas. Dichos espacios de tiempo se consideran *largos*.

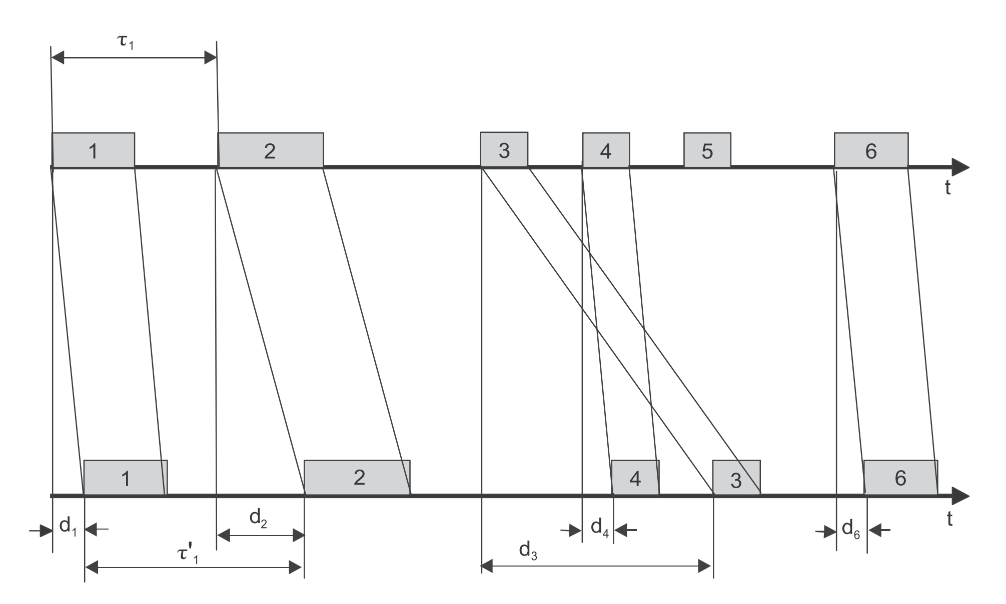


FIGURA 6.2 Transmisión de paquetes en una red real.

Existen dos grupos de características estadísticas relacionadas con el desempeño de la red:

- Características de los retardos de los paquetes.
- Características de la velocidad de la información.

6.3.2 Características de los retardos de los paquetes

El famoso **histograma de distribución** de una variable aleatoria es la herramienta principal de la estadística. En nuestro caso, la variable aleatoria por evaluar es el *retardo en la entrega de paquetes*.

Suponga que hemos medido el retardo de entrega de cada paquete y almacenado los resultados. Para obtener el histograma de distribución, tenemos que dividir todo el rango de posibles retardos en varios intervalos y calcular cuántos paquetes de la secuencia caben dentro de cada intervalo. Como resultado de lo anterior, obtenemos el histograma que se muestra en la figura 6.3. En este ejemplo, todos los valores de retardo entran en el rango de 25 a 75 mseg. La red introduce un retardo fijo igual a 25 mseg, relacionado con la propagación de la señal y el almacenamiento de paquetes. Hemos dividido este rango en seis intervalos; en consecuencia, podemos usar los seis números siguientes para caracterizar la red: *n1*, *n2*, *n3*, *n4*, *n5* y *n6*. Esta forma de representación es significativamente más compacta. Mientras el número de intervalos en los que dividamos el rango completo de valores sea menor, el número de valores utilizados para caracterizar las mediciones también será menor. Sin embargo, es necesario observar un equilibrio razonable entre nuestro afán de reducir el número de intervalos a un valor mínimo y la densidad de información de la característica.

El histograma de retardos proporciona una representación magnífica del desempeño de la red. Mediante su uso, podemos evaluar qué retardos son probables y cuáles no lo son. A medida que el tiempo durante el cual acumulamos datos para crear el histograma es mayor, el diagrama resultante reflejará con más precisión las tendencias de comportamiento de la red. Esto significa que será posible predecir el comportamiento de la red de manera

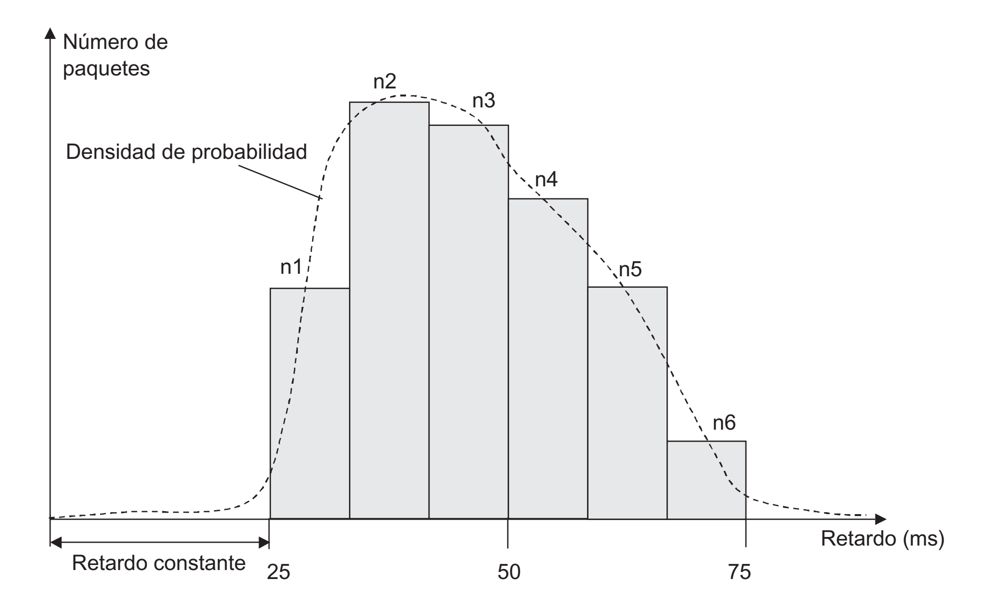


FIGURA 6.3 Histograma que muestra la distribución de retardos.

más precisa (con mayor nivel de probabilidad). Por ejemplo, mediante el uso de la gráfica de barras que se muestra en la figura 6.3, es posible afirmar que el retardo en la entrega de paquetes no excederá de 50 mseg con una probabilidad de 0.6. Para obtener este valor, utilizamos el número total de paquetes para los que los retardos de entrega caen en todos los intervalos menores a 50 mseg y dividimos este valor entre el número total de paquetes. En otras palabras, calculamos el porcentaje de paquetes para los cuales los retardos de entrega no exceden de 50 mseg.

Si aumentamos el número de intervalos y el tiempo de supervisión, en el límite obtendremos una función continua conocida como **densidad de distribución de retardo de paquetes** (en la figura 6.3 se muestra con una línea punteada). A partir de la teoría de probabilidad se sabe que para determinar la probabilidad de una variable aleatoria tomando uno de los valores de un rango específico, es necesario calcular una integral de esta función dentro de los límites inferior y superior del rango especificado. En otras palabras, necesitamos calcular un área de la figura limitada por la curva de distribución y el eje X dentro del rango especificado.

La característica más importante de las redes de conmutación de paquetes es que muchas de sus características son de naturaleza *estadística* (probabilidad). No podemos garantizar que dichas características, en determinado momento, tengan valores específicos predefinidos, sino sólo podemos afirmar que dichos eventos tienen una probabilidad específica, pues los procesos de transmisión de datos en las redes de conmutación de paquetes son *aleatorios* por naturaleza.

Consideremos algunas otras características de retardo que se utilizan con frecuencia en la práctica:

- **Retardo promedio (D):** se expresa como la suma de todos los retardos (d_i) dividida entre el número total de mediciones (N):

$$D = \frac{\sum_{i=1}^{N} d_i}{N} \tag{6.1}$$

- **Jitter**[1] **(J):** representa la desviación promedio de retardos a partir del retardo promedio:

$$J = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(d_i - D)^2} \qquad (6.2)$$

Tanto el retardo promedio como el *jitter* se miden en segundos. Como es obvio, si todos los valores de retardo d_i son iguales, $D = d_i$ y $J = 0$ (es decir, no hay *jitter*).

- **Coeficiente de variación (C_v):** es un valor adimensional igual al cociente del *jitter* entre el retardo promedio:

$$C_v = \frac{J}{D} \qquad (6.3)$$

El coeficiente de variación caracteriza el tráfico sin relacionarlo con los valores absolutos de la escala de tiempo. El flujo sincrónico ideal (es decir, una corriente) siempre tendrá una desviación estándar de 0. Si el coeficiente de variación es igual a 1, el tráfico será de ráfagas.

- **Retardo máximo:** es el valor que no deberán exceder los retardos de los paquetes con cierta probabilidad predefinida. Hasta hace muy poco tiempo, para determinar dichos valores se utilizaba el histograma de retardos. Para obtener una evaluación que definitivamente sirva como evidencia de la calidad de la operación de la red, tiene sentido especificar una alta probabilidad, por ejemplo: 0.95 o 0.99. Si una compañía le dice a un usuario que la red asegura un nivel de retardo de 100 mseg con una probabilidad de 0.5, será poco probable que el cliente quede satisfecho, ya que éste no sabrá nada respecto al nivel de retardo de la mitad del número total de paquetes.
- **Máxima variación del retardo:** es el valor máximo que la desviación del retardo no excede de su valor promedio con una probabilidad predefinida.
- **Tiempo de respuesta de la red:** es una característica integral de la red desde el punto de vista del usuario. A esta característica se refieren los usuarios cuando dicen que la red opera a una velocidad lenta en determinado día.

  El tiempo de respuesta es el periodo entre la generación de la solicitud del usuario de algún servicio de la red y la recepción de la respuesta a dicha solicitud. El tiempo de respuesta de la red puede representarse como la suma de varios componentes (figura 6.4). En general, ésta incluye el tiempo de generación de la solicitud en la computadora cliente (t_{cliente}), el tiempo necesario para transmitir la solicitud desde el cliente hasta el servidor a través de toda red (t_{red1}), el tiempo necesario para procesar solicitudes del lado del servidor (t_{servidor}), el tiempo necesario para transmitir las respuestas del servidor hacia el cliente a través de la red (t_{red2}), y el tiempo necesario para procesar las respuestas del servidor en la computadora cliente (t_{cliente2}). El tiempo de respuesta de la red caracteriza a la red como un todo. Entre otros factores, depende de la calidad de la operación del hardware y software del servidor.

- **Tiempo del viaje redondo** (**RTT**): es el tiempo neto necesario para el transporte de datos desde el nodo de origen hasta el nodo de destino y de regreso, sin tener en cuenta el tiempo requerido por el nodo de destino para generar una respuesta. Esto significa que:

$$\text{RTT} = t_{\text{red1}} + t_{\text{red2}} \qquad (6.4)$$

[1] El término *jitter* es del medio de las redes. El vocablo matemático de este valor es *desviación estándar*.

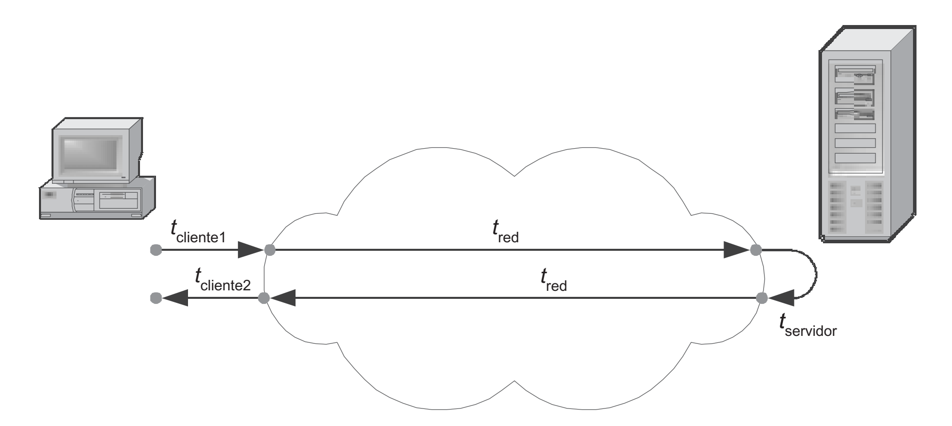


FIGURA 6.4 Tiempo de respuesta de la red y tiempo del viaje redondo.

En contraste con el tiempo de respuesta de la red, el cual caracteriza la red como un todo, el RTT permite la evaluación de las características de transporte de la red de manera individual y, en consecuencia, da la oportunidad de mejorarlas.

El RTT es una característica útil, siempre y cuando los tiempos de transmisión en cada dirección sean diferentes. De manera similar a los retardos en una sola dirección, el RTT puede evaluarse mediante su valor promedio y su valor máximo (con una probabilidad predefinida).

Según el tipo de aplicación, es posible utilizar un conjunto específico de características de retardo. Considere, por ejemplo, la difusión de música a través de Internet. Como este servicio no es interactivo, tolera retardos significativos de los paquetes individuales, a veces de varios minutos; sin embargo, la variación de retardos no deberá exceder el rango de 100 a 150 mseg; de otra forma, la calidad de la música se degradará de manera significativa. Como consecuencia, en este caso los requerimientos de la red deben incluir limitaciones en cuanto a la variación del retardo promedio o respecto al valor máximo de la variación del retardo.

6.3.3 Características de la velocidad de información

La **velocidad de información** siempre se mide en algún espacio de tiempo como el resultado de dividir el volumen de los datos transmitidos entre la duración de dicho espacio. Esto significa que la velocidad de la información siempre representa un valor promedio; no obstante, dependiendo de la duración del intervalo de la medición, esta característica se conoce con nombres diferentes.

La **velocidad de información sostenida** (**SIR**) se define como un tiempo relativamente prolongado, lo suficiente para permitirnos hablar de comportamiento estable de la velocidad de la información. Es necesario especificar en el SLA el periodo de supervisión para este valor (10 segundos, por ejemplo). Esto significa que cada 10 segundos se mide la velocidad del flujo de información y se compara con el requerimiento. Si no se llevan a cabo dichas mediciones de control, esto demeritaría la posibilidad del usuario para presentar una queja al proveedor en caso de un conflicto. Suponga que durante determinado día del mes, el proveedor no transmitió el tráfico del usuario, pero en los demás días permitió que el usuario excediera la cuota predefinida, de tal forma que la velocidad promedio mensual está dentro de los límites acordados. En estas condiciones, solamente el control regular sobre la velo-

cidad de la información facilitará que los usuarios hagan valer sus derechos. El SIR es una característica a mediano plazo. El término v**elocidad de información comprometida** (**CIR**) es sinónimo del SIR.

La **velocidad de información pico** (**PIR**) es la velocidad máxima que se le permite alcanzar, a la velocidad de tráfico del usuario, durante el tiempo corto *T* acordado.

Dicho periodo se conoce generalmente con el nombre de **periodo de ráfaga**. Como es obvio, cuando se transmite tráfico, es posible hablar de este valor solamente con cierto nivel de probabilidad; por ejemplo, el requerimiento de esta característica puede formularse como sigue: la velocidad de información no deberá exceder 2 Mbps durante 10 mseg, con una probabilidad de 0.95. Con mucha frecuencia, se omite el valor de probabilidad, pues se asume que está muy cercano a 1. El PIR es una característica de corto plazo.

El PIR permite evaluar la habilidad que tiene una red para soportar cargas características del tráfico en ráfagas y que resultan en la presencia de congestión en la red. Si el LSA estipula el SIR y el PIR, los periodos de ráfagas deben estar acompañados de tiempos de relativa *calma*, cuando la velocidad caiga por debajo del valor promedio. Si éste no es el caso, la velocidad de información promedio no corresponderá al valor acordado.

El **tamaño de la ráfaga** (designado generalmente como *B*) se utiliza para evaluar la cantidad de memoria del switch que se requiere para el almacenamiento temporal de datos durante periodos de congestión. Tal tamaño es igual al volumen total de datos que llega al switch, durante el periodo de carga.

$$B = \text{PIR} \times T \qquad (6.5)$$

En el capítulo 3 se mencionó otro parámetro de la velocidad de tráfico: **coeficiente de ráfagas en el tráfico,** a menudo llamado también **estado de ráfagas**. Este coeficiente ha sido definido como el cociente entre la velocidad promedio de tráfico medido en un espacio largo de tiempo y la velocidad máxima medida en un periodo pequeño. La incertidumbre de los espacios de tiempo hace que el coeficiente de ráfagas sea una *característica cualitativa* de la naturaleza del tráfico.

La velocidad de transmisión de datos puede medirse entre cualquier par de interfaces de red: entre la computadora del cliente y el servidor, entre los puertos de entrada y salida del ruteador, etc. Para analizar y poner a tono la red, es de utilidad saber los anchos de banda de los elementos específicos de la misma. Es importante observar que, debido al carácter secuencial de la transmisión de datos por parte de los elementos de la red, un ancho de banda de cualquier trayectoria de red compuesta será igual a la del elemento de la trayectoria que tenga el ancho de banda *mínimo*. Por lo tanto, la máxima velocidad de transmisión de datos está siempre limitada por los elementos que tengan un ancho de banda mínimo. Para aumentar el ancho de banda de la ruta compuesta, es necesario primero poner atención en los elementos más lentos, conocidos como **cuellos de botella**.

6.4 CONFIABILIDAD

PALABRAS CLAVE: confiabilidad, disponibilidad, relación de paquetes perdidos, tiempo medio entre fallas, probabilidad de fallas, tolerancia a fallas, redundancia, rutas alternas, protocolo orientado a la conexión, reconocimiento positivo, reconocimiento negativo, método de la fuente desocupada, método de la ventana deslizante y tamaño de ventana.

Para describir la confiabilidad del servicio, a menudo se utilizan las características siguientes:

- Porcentaje de pérdida de paquetes en el flujo total.
- Disponibilidad del servicio.

Ambas características describen la confiabilidad del servicio de transporte desde el punto de vista del usuario. La diferencia entre ellos es que caracterizan la confiabilidad en rangos de tiempo diferentes. La primera característica es el corto plazo y la segunda el mediano o largo plazo.

6.4.1 Características de la pérdida de paquetes

Esta característica se define como la relación entre el número de paquetes perdidos y el número total de paquetes transmitidos:

$$\textbf{Relación de paquetes perdidos} = N_L/N \quad (6.6)$$

Aquí, N es igual al número total de paquetes transmitidos durante un tiempo específico y N_L es igual al número de paquetes perdidos durante el mismo tiempo.

6.4.2 Disponibilidad y tolerancia a fallas

Para describir la confiabilidad de los dispositivos individuales existen características de confiabilidad, como el *tiempo medio entre fallas (MTBF)*, *la probabilidad de fallas* y *la velocidad de fallas*; sin embargo, estos parámetros son adecuados solamente para evaluar la confiabilidad de elementos y dispositivos simples, los cuales se vuelven inútiles cuando falla cualquiera de sus componentes. Los sistemas complejos formados por muchos componentes pueden no tener utilidad alguna si falla uno de ellos.

En esta relación se utiliza otro conjunto de características para evaluar la confiabilidad de sistemas complejos.

La **disponibilidad** es la relación entre el tiempo durante el cual el sistema o servicio conserva su utilidad y el tiempo de vida total del sistema. La disponibilidad es una característica estadística de largo plazo. Sus intervalos típicos de medida son día, mes o año. El equipo de comunicaciones de las redes telefónicas es un ejemplo de un sistema de alta disponibilidad, ya que los mejores especímenes están caracterizados por la disponibilidad de *cinco nueves*. Esto significa que la disponibilidad de dicho equipo es de 99.999%, que corresponde a un poco más de cinco minutos al año de falla del sistema. Tanto el equipo como los servicios de las redes de datos se esfuerzan en alcanzar dicho grado de disponibilidad; sin embargo, el límite de *tres nueves* ya se ha logrado.

La disponibilidad del servicio representa una característica universal utilizada por los usuarios finales y por los proveedores de servicio.

Otra característica utilizada para evaluar la confiabilidad de sistemas complejos es la **tolerancia a fallas**, la cual es la capacidad del sistema para esconder fallas de componentes específicos del sistema a los usuarios.

Por ejemplo, si el switch está equipado con dos equipos de conmutación que trabajan en paralelo, la falla de uno de tales equipos no provocará la falla total del switch. No obstante, el desempeño de este switch disminuirá, ya que procesará paquetes dos veces más despacio. En un sistema tolerante a fallas, la falla de uno de sus elementos provocará la degradación del sistema en lugar de la falla total de éste. Otro ejemplo que ilustra la implantación de la tolerancia a fallas es el uso de dos enlaces físicos para conectar los switches. En el modo de operación normal, el tráfico se transmite a través de dos enlaces a una velocidad de 2C Mbps.

Si un enlace no funciona, el sistema de tolerancia a fallas continuará transmitiendo tráfico a una velocidad de C Mbps; sin embargo, como es difícil obtener una evaluación cuantitativa de la degradación del desempeño del sistema o servicio, la tolerancia a fallas se utiliza con mucha frecuencia como una característica cualitativa.

Además, se considerarán los métodos que se utilizan para asegurar una alta confiabilidad en los servicios de transporte.

6.4.3 Rutas alternas

La disponibilidad del servicio puede mejorarse mediante el uso de dos métodos:

- El primer método implica usar *elementos de red confiables* que rara vez fallan; no obstante, este método está siempre limitado por las capacidades de la tecnología utilizadas en el proceso de fabricación de componentes electrónicos (circuitos integrados, tarjetas de circuito impreso, etcétera).
- El segundo método también es bien conocido. Se basa en la introducción de *redundancia* en el diseño del sistema: ciertos elementos clave del sistema deberán existir por duplicado, por si un elemento falla, los duplicados asegurarán la operación normal del sistema. Por lo tanto, los switches y ruteadores que trabajan en la troncal de la red están siempre equipados con unidades redundantes: fuentes de alimentación, procesadores e interfaces.

Para asegurar el nivel de disponibilidad que requiere el servicio de transporte, la red debe contar con redundancia. La forma principal para lograr esto consiste en contar con rutas alternas. La figura 6.5*a* muestra un ejemplo de una red sin rutas alternas para la transmisión de tráfico entre los nodos A y B. Por lo tanto, este diseño de red no proporciona tolerancia a fallas y el proveedor de servicio debe depender en la capacidad de tolerancia a fallas de los diferentes elementos de la red: enlaces de datos e interruptores instalados en la ruta desde el nodo A hasta el B.

La figura 6.5*b* muestra una red que transmite tráfico entre el nodo A y el B mediante el uso de dos rutas. En el caso de una falla en el equipo a lo largo de una de las rutas, se puede utilizar la segunda ruta, permitiendo que la red continúe ofreciendo servicio a sus clientes; sin embargo, la conmutación de una ruta a la otra toma cierto tiempo. Durante algunos periodos de transmisión, se pueden presentar pérdidas en el tráfico de los usuarios. Por ende, reducir este tiempo es uno de los objetivos principales de las técnicas utilizadas para asegurar la tolerancia a fallas de la red.

Existen varios métodos de uso de rutas alternas en la red:

- *La red determina la ruta alterna solamente después de una falla en la ruta principal.* Esto significa que sólo se especifica una ruta en las tablas de direccionamiento de los switches de la red por cada flujo de información. Después de una falla en un enlace de comunicaciones o en un switch en la ruta de este flujo, los switches de la red utilizan un protocolo especial de enrutamiento para buscar una ruta alterna. En general, esto toma décimas de segundo o varios minutos, dependiendo del tamaño de la red y la complejidad de su topología. Éste es el método más lento para usar rutas alternas. Durante el periodo de transición, las pérdidas de los datos de usuario son inevitables.
- *La red busca dos rutas con antelación y las utiliza*, creando así un flujo invisible redundante al usuario. A la salida de la red, se selecciona sólo un flujo y los datos provenientes de éste se transfieren al usuario. Por lo tanto, una de las rutas se considera la ruta principal y la otra la de respaldo. Cuando falla la ruta principal, el usuario recibe los datos a través de la ruta de respaldo. Este método es el más rápido, ya que asegura el QoS más

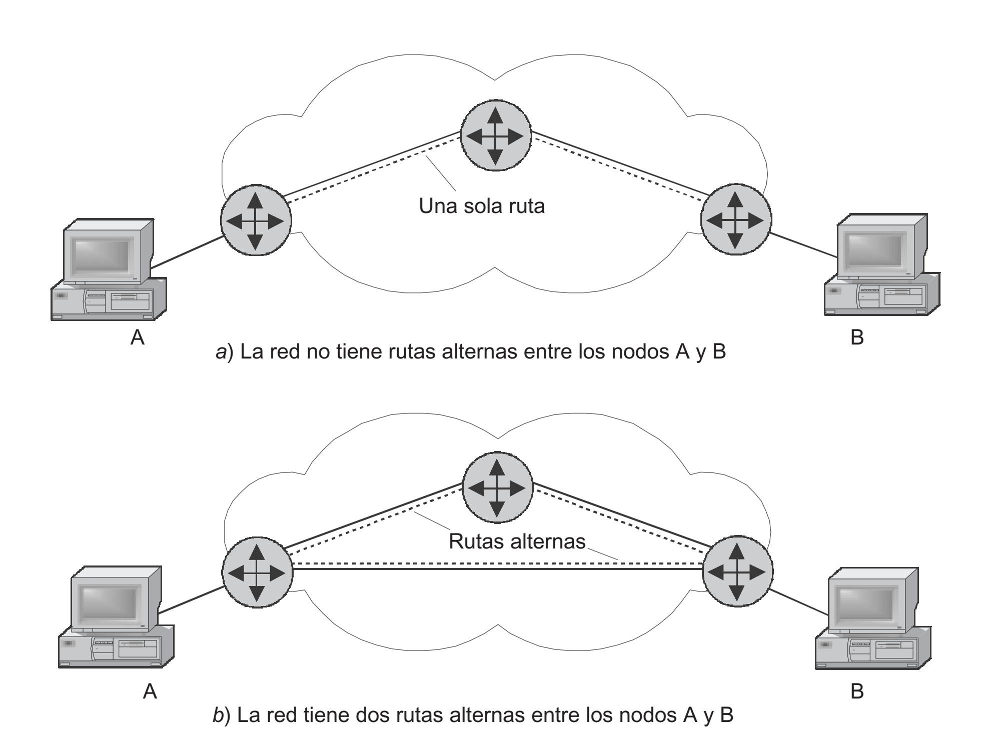


FIGURA 6.5 Rutas alternas.

elevado del flujo del usuario; empero, éste se encuentra relacionado con altas pérdidas en el desempeño de la red, pues ésta transmite dos flujos en vez de uno. Este método se utiliza normalmente para dar servicio a un pequeño número de flujos de datos de gran importancia que requieren un alto nivel de disponibilidad del servicio.

- *La red busca dos rutas con antelación, pero solamente utiliza una de ellas.* Cuando la ruta principal falla, la transición hacia la alterna es mucho más rápida que cuando se usa el primer método, ya que el sistema no necesita gastar tiempo en buscar una ruta alterna. Este método es mucho más económico que el segundo; sin embargo, las pérdidas de datos son mayores que cuando se emplea el segundo método, porque los datos que se enviaron a través de la ruta que falló se perdieron. Se requiere cierto tiempo para que el primer switch instalado a lo largo de la ruta del flujo sepa que hubo una falla en la red y que la ruta principal ya no es válida.

Las redes de computadoras utilizan principalmente el primer y tercer métodos para el enrutamiento alterno. Las tecnologías basadas en el segundo principio (dos rutas activas) se usan sólo en las redes que necesitan asegurarse de contar con un grado mayor de confiabilidad. El segundo método se emplea en las redes de transmisión de alta velocidad, las cuales ofrecen una infraestructura de enlaces muy confiable para el tráfico telefónico y entre computadoras.

6.4.4 Retransmisión de datos y la ventana deslizante

Los métodos de transmisión de paquetes se utilizan cuando fallan otros métodos para asegurar la confiabilidad y los paquetes se pierden. Estos métodos requieren usar protocolos orientados a la conexión.

Para asegurarse de que es necesario retransmitir los datos, el emisor numera los paquetes que envía; por cada paquete, el emisor espera un **reconocimiento positivo** (**ACK**) del receptor. El ACK es un paquete o un campo especial dentro de un paquete de datos, el cual informa al emisor que el paquete de origen se recibió y que sus datos son correctos. Para organizar dicha numeración, se necesita un procedimiento para establecer una conexión lógica, pues éste proporciona el punto de referencia a partir del cual comienza la numeración. El periodo de espera del reconocimiento es limitado (cuando se envía cada paquete, el emisor arranca un reloj y si el reconocimiento no se recibe antes de un tiempo predefinido, se considera que el paquete se perdió). Si el destinatario recibe el paquete con información dañada, enviará un **reconocimiento negativo** (**NACK**), en el que especifica que el paquete necesita ser retransmitido.

Existen dos métodos para organizar el proceso de intercambio de reconocimientos: el método del origen libre y el de la ventana deslizante.

El **método del origen libre** requiere que el emisor envíe el paquete para esperar el reconocimiento (positivo o negativo) del receptor. El emisor puede enviar el paquete siguiente sólo después de que haya recibido el reconocimiento positivo.[2] Si el reconocimiento no se envía después de que haya terminado el tiempo de espera, o bien si se recibió un reconocimiento negativo, el paquete se considera perdido y tiene que retransmitirse. La figura 6.6*a* muestra que esta situación degrada significativamente el desempeño del intercambio de datos; en otras palabras, la utilización del enlace es muy baja. Aunque el emisor sea capaz de enviar el paquete siguiente inmediatamente después de enviar el anterior, tiene que esperar un reconocimiento. La degradación del desempeño de este método de corrección de errores es particularmente observable en enlaces de baja velocidad (es decir, en WAN).

El segundo método de corrección de errores se conoce como **método de ventana deslizante**. Para incrementar la velocidad de datos, este procedimiento permite que el emisor transmita un número específico de paquetes de modo continuo, es decir, a la máxima velocidad posible, sin recibir reconocimiento positivo de dichos paquetes. El número de paquetes que pueden transmitirse de esta forma se conoce como **tamaño de ventana**. La figura 6.6b muestra este método para una ventana formada por W paquetes.

En el momento de comenzar, cuando no se han enviado paquetes, la ventana define el rango de paquetes con los números del 1 al W, inclusive. El emisor comienza a transmitir paquetes y recibir reconocimientos. Por simplicidad, suponga que los reconocimientos llegan en el mismo orden que los paquetes a los que corresponden. En el instante t_1, después de recibir el primer reconocimiento (ACK1), la ventana se mueve una posición, definiendo un nuevo rango: del 2 al $(W + 1)$.

El proceso de envío de paquetes y recepción de reconocimientos son del todo independientes. Considere un instante arbitrario, t_n, en el que el origen ya recibió el reconocimiento de todos los paquetes numerados del 1 al n. La ventana se ha desplazado hacia la derecha y ha definido que se permita la transmisión de un nuevo rango de paquetes. Dicho rango va desde $(n + 1)$ a $(W + n)$. Todo el conjunto de paquetes desde el origen puede clasificarse en los grupos siguientes (consulte la figura 6.6*b*):

- *Los paquetes con números del 1 al n* han sido enviados y ya se recibieron los reconocimientos correspondientes, lo cual significa que están ubicados fuera del límite izquierdo de la ventana.

[2] Por brevedad, nos referiremos a los reconocimientos positivos simplemente como reconocimientos.

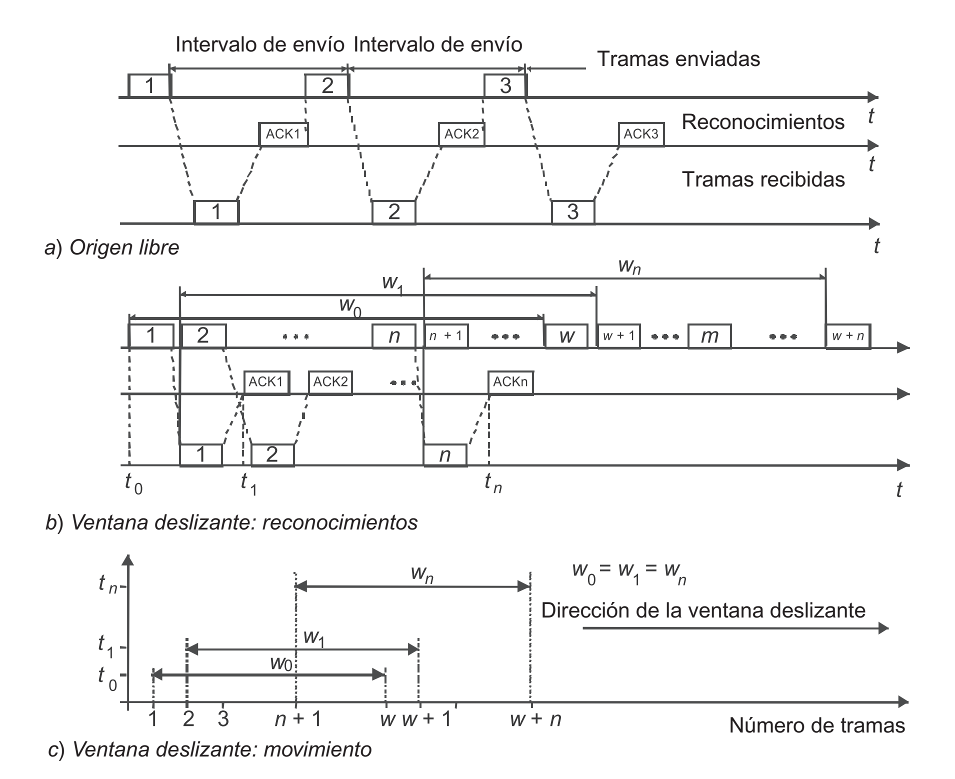


FIGURA 6.6 Métodos para restablecer paquetes dañados o perdidos.

- *Los paquetes del número (n + 1) al (W + n)* están ubicados dentro de los límites de la ventana. Dichos paquetes pueden enviarse sin tener que esperar un reconocimiento. Este rango puede subdividirse en los intervalos siguientes:
  - Paquetes con números del *(n + 1)* al *m*, los cuales ya se enviaron; sin embargo, sus reconocimientos no se han recibido todavía.
  - Paquetes numerados desde del *m* al *(W + n),* los cuales pueden enviarse pero eso todavía no se hace.
- *Todos los paquetes con números mayores a (W + n)* están ubicados fuera de la frontera derecha de la ventana y, por lo tanto, no pueden enviarse todavía.

El proceso de deslizar la ventana a lo largo de la secuencia de números de paquete se muestra en la figura 6.6*c*. Aquí, t_0 es el instante inicial y t_1 y t_n son los tiempos de llegada de reconocimientos del primero y el enésimo paquete, respectivamente. Cada vez que llega un reconocimiento, la ventana se desliza a la derecha y su tamaño permanece inalterado e igual a *W*.

Por lo tanto, cuando se envía un paquete con número igual a *n*, el espacio de tiempo se establece en el nodo de origen. Si durante este tiempo el reconocimiento del paquete *n* no llega, dicho paquete se considerará perdido y tiene que retransmitirse.

Si el flujo de reconocimientos llega de forma regular, de tal manera que el emisor siempre cuente con paquetes que tengan derecho a ser enviados, la velocidad de intercambio alcanzará el valor máximo posible para un enlace específico y para determinado protocolo adoptado. A partir de la descripción del método de la ventana deslizante, es evidente que el método del origen libre representa un caso particular de este algoritmo para el cual el tamaño de ventana es igual a 1.

Algunas implementaciones del algoritmo de la ventana deslizante no requieren que el receptor envíe reconocimientos por cada paquete recibido correctamente. Si no existen espacios entre los paquetes recibidos, el receptor puede enviar el reconocimiento sólo del último paquete recibido y dicho reconocimiento será interpretado por el emisor como una señal de que todos los paquetes anteriores también fueron entregados con éxito.

Algunos métodos utilizan reconocimientos negativos, los cuales se dividen en dos categorías: grupales y selectivos. Los reconocimientos grupales contienen el número del paquete desde el cual es necesario comenzar a retransmitir todos los paquetes enviados por el emisor. El reconocimiento negativo selectivo requiere la retransmisión de un solo paquete.

El método de la ventana deslizante tiene dos parámetros que pueden influir de manera significativa en la eficacia del intercambio de datos entre el emisor y el receptor. Éstos son el tamaño de ventana y el valor del tiempo de descanso durante el cual el emisor espera el reconocimiento. La selección del valor del tiempo de descanso depende de los retardos de los paquetes.

En las redes confiables, en las que los paquetes rara vez se pierden o dañan, es necesario aumentar el tamaño de la ventana con el fin de incrementar la velocidad de intercambio de datos. Si se utiliza este método, el emisor enviará paquetes con pausas más pequeñas. En las redes no confiables, el tamaño de ventana debe disminuirse, ya que en condiciones de pérdidas frecuentes, daño de datos o ambos, el volumen de paquetes retransmitidos aumenta de forma considerable. Cuando esto sucede, el ancho de banda se emplea de forma muy ineficiente y el ancho de banda útil de la red disminuye.

El tamaño de la ventana puede ser un parámetro *constante* en este algoritmo, lo cual significa que se selecciona en el momento de establecer la conexión y no varía durante toda la sesión.

También existen versiones *adaptables* de este algoritmo cuando el tamaño de la ventana cambia durante la sesión de acuerdo con la confiabilidad y la carga de la red. En condiciones de baja confiabilidad de la red y carga elevada, el emisor reduce el tamaño de la ventana, con la intención de encontrar el modo óptimo de transmitir datos. La confiabilidad de la red en dichos algoritmos está determinada por síntomas de pérdida de paquetes, como el término del tiempo de descanso para el reconocimiento positivo o la llegada de reconocimientos duplicados en ciertos paquetes. La llegada de reconocimientos duplicados sirve como evidencia de que el tiempo de descanso del paquete siguiente en el nodo de destino ha terminado, y éste solicita la retransmisión de ese paquete.

Los nodos de destino también pueden cambiar el tamaño de la ventana. Esto puede suceder si el nodo de destino se sobresatura y no es capaz de procesar todos los paquetes que llegan a tiempo. Este problema se evaluará más adelante en la sección "Retroalimentación" del capítulo 7, cuando se estudien los problemas relacionados con la eliminación de congestión en las redes.

Existen también implementaciones del algoritmo de la ventana deslizante que utilizan el número de bytes como tamaño de ventana en vez de usar el número de paquetes. El protocolo TCP representa el ejemplo mejor conocido de dicho método.

El método de la ventana deslizante es más difícil de establecer que el método del origen libre, ya que el emisor debe almacenar en su memoria todos los paquetes para los cuales no ha recibido todavía reconocimiento positivo. Además, es necesario rastrear varios parámetros de este algoritmo, incluidos el tamaño de ventana, los números de los paquetes para los cuales se ha recibido reconocimiento y los números de paquetes que pueden ser transmitidos antes de recibir un nuevo reconocimiento.

6.5 SEGURIDAD

PALABRAS CLAVE: herramientas para la seguridad de computadoras, herramientas para la seguridad de redes, firewalls, red privada virtual (VPN), confidencialidad, disponibilidad de la información, autentificación, integridad, encriptado, sistema criptográfico, firma digital, autorización de la identificación, auditoría, y tecnología de canal protegido.

Las redes de computadoras representan formas magníficas de acceder a distintos tipos de información y son excelentes herramientas de comunicación; sin embargo, también tienen un lado negativo. Éste se manifiesta en la forma de amenazas potenciales a la integridad y confidencialidad de la información que usted confía a la red. Por ejemplo, las compañías que tienen conexiones permanentes a Internet suelen sufrir ataques por parte de intrusos a sus recursos de información. Los usuarios individuales de Internet que establecen conexiones conmutadas también se encuentran expuestos a dichos ataques. La información almacenada en sus computadoras puede ser víctima de gusanos de correo electrónico o vulnerabilidades típicas de los sistemas de mensajería instantánea, como el ICQ.

ALGUNAS ESTADÍSTICAS

En la edición del reporte anual Issues and Trends: 2002 CSI/FBI Computer Crime and Security Survey, publicado en abril de 2002, se reportó un crecimiento agudo del delito en las computadoras. Alrededor de 90% de los encuestados (principalmente empleados de grandes compañías y organizaciones gubernamentales) reportaron que durante los 12 meses anteriores se presentaron incidentes de seguridad en sus organizaciones. Cerca de 80% de los encuestados registraron pérdidas financieras provocadas por estas violaciones a la seguridad y 44% evaluaron las pérdidas en forma cuantitativa. De acuerdo con los datos que reportaron, la pérdida financiera total excedió la cantidad de 455 millones de dólares.

Los intrusos que quieran obtener acceso sin autorización a la información de las computadoras o destruirla pueden usar Internet y redes corporativas. Nadie puede garantizar que algún empleado descontento no quiera hacer mal uso de sus privilegios intentando acceder a documentos que no tenga derecho a leer. También es posible intentar destruir información (como eliminar archivos o provocar que las computadoras funcionen mal).

Obviamente, los usuarios de la red desean proteger su información contra este tipo de incidentes. El nivel de seguridad de la información del usuario de la red es otro rasgo importante con la que la red debe contar. Dicho nivel no es una característica cuantitativa; por el contrario, sólo puede evaluarse de manera cualitativa, por ejemplo: de nivel bajo, medio o alto. Normalmente, para otorgarle un nivel adecuado al nivel de seguridad de la red, es necesario consultar a expertos.

6.5.1 Seguridad en computadoras y redes

La gama de herramientas para la protección de información puede dividirse en dos clases:

- **Herramientas de seguridad en computadoras** diseñadas para proteger recursos de información internos ubicados dentro de una LAN o en una computadora independiente de un usuario final.

- **Herramientas de seguridad de la red** diseñadas para proteger la información que se transmite a lo largo de la red.

Las funciones de seguridad de estas dos clases difieren de manera significativa. En la primera, es necesario proteger contra el acceso no autorizado a todos los recursos dentro de la LAN, incluidos hardware (servidores, arreglos de discos y ruteadores), software (sistemas operativos, DBMS, servicios de correo, etc.) y datos almacenados en archivos y procesados en RAM. Para lograr lo anterior, es necesario inspeccionar todo el tráfico entrante a la red local desde una red pública (por el momento, Internet es la red pública por excelencia) y tratar de evitar el acceso externo a cualquier información que pueda ayudar a los intrusos a abusar de los recursos que contengan información confidencial.

La herramienta de protección de este tipo que se utiliza con mayor frecuencia se llama **firewall** y se instala entre todas las conexiones de la red interna hacia Internet. Los firewalls representan los filtros de la interred que se encargan de verificar el intercambio de mensajes a todos los niveles de protocolos y no admiten que exista tráfico sospechoso en la red que se protege.

Los firewalls también pueden utilizarse dentro de la red para proteger una subred de otra. Esta configuración puede ser necesaria en grandes compañías con departamentos independientes. Dichos problemas también pueden resolverse mediante el uso de herramientas de seguridad incluidas en los sistemas operativos y en las aplicaciones (por ejemplo: un sistema de administración de bases de datos), así como con el hardware de seguridad incluido.

En la segunda clase es necesario proteger la información que reside fuera de los límites o fuera del alcance. Generalmente, esta información viaja a través de las redes de los proveedores en forma de paquetes IP. En la actualidad, Internet es usada por la mayoría de las compañías no sólo como una poderosa fuente de información distribuida a lo largo de un gran número de sitios web, sino también como un ambiente de transporte relativamente barato que permite a la red de la casa matriz conectarse con las redes de distintos departamentos. Asimismo, facilita la conexión de múltiples usuarios móviles y de los que residen fuera de la ciudad. En la mayoría de los casos, es de vital importancia asegurar que la información transmitida por medio de Internet no vaya a ser dañada, destruida o vista por una tercera instancia no autorizada a hacerlo. Hasta el momento, las herramientas de **red privada virtual** (**VPN**) se utilizan con mucha frecuencia para este propósito.

Las computadoras independientes pueden protegerse de manera eficaz contra intrusiones externas, si se utilizan varias herramientas. Por ejemplo, se puede guardar bajo llave el teclado o quitar el disco duro y guardarlo en un lugar seguro. Las computadoras que forman parte de la red, por definición, no pueden estar aisladas totalmente del mundo exterior, pues tienen que comunicarse con otras computadoras, algunas de las cuales están localizadas a una distancia considerable entre sí. Por lo tanto, garantizar la seguridad en las redes es una tarea mucho más complicada, comparada con las máquinas independientes. Las situaciones en las que usuarios remotos establecen conexiones lógicas hacia su computadora se consideran estándar, siempre y cuando su computadora esté conectada a la red. Garantizar la seguridad en esta condición implica tener control de estas conexiones —cada usuario de la red debe tener derechos de acceso definidos de manera estricta a la información almacenada en cada computadora local, derechos de acceso a los dispositivos periféricos y privilegios para llevar a cabo acciones administrativas específicas en cada computadora conectada a la red—.

Además de los problemas generados por la posibilidad de un acceso remoto a las computadoras de la red, las redes están expuestas a otro tipo de amenazas: el rastreo y análisis de mensajes transmitidos a lo largo de la misma y la generación de tráfico falso. Gran parte

de las herramientas de seguridad de redes están diseñadas para evitar este tipo de incidentes de seguridad.

Los aspectos de seguridad en redes son especialmente importantes ahora, cuando la mayoría de las compañías están migrando de líneas arrendadas a redes públicas (Internet, Frame Relay) al diseñar sus redes corporativas.

6.5.2 Confidencialidad, integridad y disponibilidad de los datos

Un sistema de información seguro es aquel que, en primera instancia, protege los datos contra el acceso no autorizado; en segundo lugar, siempre está disponible para brindar los datos necesarios a usuarios autorizados; y en tercer lugar, almacena de manera confiable la información y garantiza que ésta no varíe. Por lo tanto, un sistema seguro se caracteriza por su confidencialidad, disponibilidad e integridad.

- **Confidencialidad:** es la garantía de que los datos estarán a disposición solamente de los usuarios que estén autorizados para acceder a esta información. Se conocen con el nombre de *usuarios autorizados*.
- **Disponibilidad de la información:** es la garantía de que los usuarios autorizados siempre tendrán acceso a los datos que necesiten.
- **Integridad:** es la garantía de que los datos siempre conservarán sus valores correctos. Para lograr esto, se niega el acceso a usuarios no autorizados, con lo cual se evita que éstos cambien, modifiquen, eliminen o generen nuevos datos.

El objetivo de un intruso podría consistir en violar todos los componentes de la seguridad de la información —disponibilidad, integridad y confidencialidad—. Las necesidades de seguridad pueden cambiar en función de los objetivos del sistema, el tipo de datos que se usen y las posibles amenazas. Es difícil imaginar un sistema para el que las propiedades de integridad y disponibilidad no sean importantes; sin embargo, la propiedad de confidencialidad no es obligatoria en todos los casos. Por ejemplo, si usted publica información en un sitio web en Internet y desea que se encuentre disponible a la mayor audiencia posible, no será necesaria la confidencialidad. Empero, los requerimientos de integridad y disponibilidad conservarán su importancia.

Si usted no toma las medidas adecuadas para garantizar la integridad de los datos, el intruso podría modificar los datos almacenados en su servidor y provocar daños en su compañía. Los usuarios maliciosos podrían, por ejemplo, introducir algunos cambios en la lista de precios publicada en el servidor web, los cuales reducirían el potencial competitivo de su compañía. También podrían dañar los códigos del software sin costo que proporciona su compañía, lo cual provocaría un daño a la reputación de su negocio.

Garantizar la disponibilidad de los datos en este ejemplo no es algo de menor importancia. Después de realizar inversiones financieras significativas en la creación y soporte de un sitio web, una compañía tiene el derecho a esperar un retorno de su inversión en la forma de un número de clientes mayor, un crecimiento en las ventas, etc. Sin embargo, el intruso puede llevar a cabo un ataque que tenga como consecuencia que los datos publicados en el servidor no estén a disposición de los usuarios para los cuales la información iba dirigida. Algunos ejemplos de ataques consisten en saturar al servidor con paquetes IP que contengan una dirección de regreso incorrecta. Dichos paquetes son la lógica interna de este protocolo, pueden provocar tiempos muertos y, en consecuencia, hacer que el servidor no esté disponible para las solicitudes de todos los usuarios. Este ataque representa un caso particular de ataque de negación del servicio (DoS).

NOTA *Los conceptos de confidencialidad, disponibilidad e integridad no solamente se pueden definir en relación con otros recursos de la red de datos, como los dispositivos periféricos y las aplicaciones. Por ejemplo, el acceso sin restricciones a una impresora podría permitir a un intruso obtener copias de los documentos que se estuviesen imprimiendo, cambiar los valores de los parámetros de la impresora o, más aún, provocar que falle. La propiedad de confidencialidad respecto a las impresoras, puede interpretarse como sigue: sólo aquellos usuarios autorizados para utilizar el dispositivo podrán acceder a él; además, aun si se trata de los usuarios autorizados, éstos solamente podrán realizar las operaciones que tienen permitidas. La propiedad de disponibilidad, en este caso, significa que el dispositivo debe estar listo para usarse en cualquier momento. En cuanto a la integridad, ésta puede definirse como la invariabilidad de los parámetros que se definieron para un dispositivo específico.*

6.5.3 Servicios de seguridad en las redes

Con frecuencia los diferentes productos de software y hardware diseñados para la protección de datos utilizan formas, técnicas y soluciones muy similares. A continuación se consideran las más importantes.

- **Encriptado:** es la base de los servicios de seguridad de la información, ya sea sistemas de autenticación o autorización, herramientas para crear canales con protección o métodos para asegurar el almacenamiento de datos. Cualquier procedimiento de encriptado que convierta la información de su forma legible (texto) a datos encriptados (texto cifrado) debe complementarse con un procedimiento de desencriptado que, si se aplica al texto cifrado, lo convierta a su forma legible. Ambos procedimientos (encriptado y desencriptado) se conocen como **sistema criptográfico**.
- **Autenticación:** evita el acceso no autorizado a la red y permite que solamente los usuarios autorizados puedan iniciar sesión en el sistema. El término *autenticación* tiene un origen latino y significa verificación del original. La lista de objetos que pueden requerir autenticación, además de los usuarios, consiste en varios dispositivos, aplicaciones e información. Por ejemplo, los usuarios que envían una solicitud a un servidor corporativo deben demostrar su autenticidad y asegurarse de que se comunican con el servidor que pertenece a la compañía. En otras palabras, tanto el cliente como el servidor deben llevar a cabo procedimientos de mutua autenticación (ésta es autenticación a nivel de aplicación). Cuando se establece una sesión de comunicaciones entre dos dispositivos, es posible que sean necesarios los procedimientos de autenticación a nivel de la capa de enlaces de datos. La autenticación de los datos significa demostrar su integridad, así como también probar que han sido recibidos de la persona que dice proporcionar dicha información. Para este propósito, se utiliza con mucha frecuencia el método de la **firma digital**. La autenticación no debe confundirse con la identificación.
- **Identificación:** significa que el usuario determina un identificador personal del sistema; autentificación es el procedimiento de verificar que el usuario es en realidad quien dice ser. En particular, cuando el usuario entra al sistema, debe proporcionar la contraseña para demostrar que es la persona a la que pertenece el identificador específico. Los identificadores de usuario son utilizados de la misma manera que los identificadores de otros objetos, como archivos, procesos y estructuras de datos y no están relacionados directamente con la seguridad.
- **Autorización:** es el procedimiento para controlar el acceso de usuarios autenticados a los recursos del sistema. Un sistema de autorización ofrece a cada usuario exactamente

los derechos que le otorgó el administrador. Además de proporcionar los derechos de acceso a archivos, directorios, impresoras, etc., un sistema de autorización debe controlar los privilegios del usuario (es decir, la posibilidad de llevar a cabo tareas específicas), como acceso local al servidor, fijar la hora del sistema, crear copias de respaldo de los datos y apagar el servidor. Un usuario autenticado al que se otorgan derechos de acceso específicos y privilegios se conoce como *usuario autorizado*.

- **Auditoría:** es el proceso de registro de todos los eventos relacionados con el acceso a los recursos protegidos del sistema en la bitácora del mismo. El subsistema de auditoría de los sistemas operativos modernos permite diferenciar eventos de interés para los administradores del sistema cuando se usa una interfase gráfica de usuario apropiada. Las herramientas de auditoría y supervisión proporcionan la posibilidad de detectar y registrar eventos de importancia relacionados con la seguridad, así como cualquier intento de crear nuevos recursos del sistema y acceder a, modificar o eliminar recursos existentes. La auditoría se utiliza para detectar cualquier intento de intrusión, incluidos aquellos que no tuvieron éxito.
- **Tecnología de canal protegido:** está diseñada para garantizar la seguridad de la transmisión de datos a través de redes públicas, como Internet. Un canal protegido implica observar los tres requerimientos siguientes:
  - Autenticación mutua de usuarios cuando establecen una conexión, la cual podrá realizarse, por ejemplo, mediante el intercambio de contraseñas.
  - Protección de mensajes transmitidos contra accesos no autorizados utilizando un canal protegido, por ejemplo, mediante la encriptación de datos.
  - Garantizar la integridad de los mensajes que llegan a través del canal protegido, lo cual puede llevarse a cabo, por ejemplo, a través de la transmisión simultánea de la firma digital.

  La tecnología de canal protegido se utiliza ampliamente en el diseño de VPN.

6.6 CARACTERÍSTICAS ÚNICAS DEL PROVEEDOR

PALABRAS CLAVE: extensibilidad, escalabilidad, administración de la red, sistema de administración de la red, capacidades de integración, red heterogénea y red integrada.

Considere las características principales que los proveedores de servicios utilizan cuando evalúan la eficiencia de sus redes. Dichas características a menudo son cualitativas.

6.6.1 Extensibilidad y escalabilidad

Los términos *extensibilidad* y *escalabilidad* suelen utilizarse como sinónimos, lo cual es incorrecto, ya que cada uno de ellos tiene un significado independiente estrictamente definido.

- **Extensibilidad:** es la posibilidad de agregar usuarios de manera relativamente sencilla, así como nuevos componentes de la red (por ejemplo, computadoras, switches, ruteadores o servicios), aumentar la longitud de los segmentos de cable de la red y reemplazar el equipo existente con dispositivos nuevos que sean más avanzados y poderosos. La facilidad de extender la red puede garantizarse a veces dentro de ciertos límites solamente. Por ejemplo, la red Ethernet basada en un solo segmento de cable coaxial delgado se caracteriza

por tener una buena extensibilidad, ya que ésta proporciona la posibilidad de conectar fácilmente nuevas estaciones de trabajo. Sin embargo, dichas redes están limitadas por el número de estaciones que se le pueden conectar, el cual no debe exceder de 40. Aunque esta red permite la conexión física de mayor número de estaciones de trabajo al segmento (hasta 100), su desempeño, en este caso, decae significativamente. La presencia de dichas limitantes es un signo de una pobre escalabilidad del sistema, aunque la extensibilidad de dicho sistema es muy buena.

- **Escalabilidad:** significa la posibilidad de aumentar de modo importante el número de nodos de la red y la longitud de los enlaces sin que se degrade el funcionamiento de la misma. Para garantizar que una red es escalable, es necesario emplear equipo adicional de comunicaciones y observar reglas especiales para su estructuración. En general, una solución escalable tiene una estructura jerárquica multicapa, la cual permite agregar nuevos elementos en cada capa jerárquica sin tener que cambiar la idea principal del proyecto. Internet es un ejemplo de una red escalable, ya que su tecnología (TCP/IP) es capaz de soportar la red a una escala mundial. La estructura organizacional de Internet, la cual se estudió en el capítulo 5, comprende varias capas jerárquicas: redes de usuario, redes ISP locales, etc., hasta las redes ISP internacionales. Las tecnologías TCP/IP, sobre las que se basa toda la red Internet, también permiten construir redes jerárquicas. El protocolo principal de Internet (IP) se basa en un modelo de dos capas. La capa inferior está diseñada por las redes individuales (redes corporativas principalmente) y la capa superior representa la interred que conecta a estas redes. En la pila de protocolos TCP/IP existe el concepto de sistema autónomo, el cual incluye todas las interredes de un solo ISP, de tal forma que el sistema autónomo representa una capa jerárquica superior. La presencia de sistemas autónomos en Internet facilita simplificar la solución al problema de la ruta racional. En primera instancia, es suficiente encontrar la ruta racional entre los sistemas autónomos y después encontrar una ruta racional por cada sistema autónomo dentro de sus fronteras.

Para garantizar una solución escalable, no solamente debe ser escalable la red en sí misma, sino también los dispositivos del troncal, ya que el crecimiento de la red no debe tener como consecuencia la necesidad constante de reemplazar equipo. Por lo tanto, los switches y ruteadores del troncal están construidos generalmente según el principio modular, el cual ofrece la posibilidad de aumentar, de forma sencilla, el número de interfases y mejorar la operación del procesamiento de paquetes.

6.6.2 Administración

La **administración de la red** es una característica cualitativa y supone la posibilidad de controlar de manera centralizada el estado de los elementos principales de la red, de detectar y resolver sus problemas, analizar su desempeño y planear su crecimiento. La administración implica la presencia de herramientas automatizadas de manejo y control dentro de la red. Dichas herramientas interactúan con el hardware y software de la red mediante el uso de protocolos de comunicaciones.

En forma ideal, un **sistema de administración de red** (**NMS**) supervisa, controla y administra cada elemento de la misma —desde los dispositivos más sencillos hasta los más complejos—. Al mismo tiempo, tal sistema considera la red como un todo, más que como un conjunto de dispositivos individuales independientes.

Un buen NMS supervisa la red y, una vez que ha detectado un problema, activa una acción específica, corrige la situación y notifica al administrador acerca del evento que ha

ocurrido y cuáles son las acciones correctivas. Al mismo tiempo, el NMS debe acumular datos con base en los cuales sea posible planear el futuro desarrollo de la red. Por último, el NMS debe proporcionar una interfase de usuario apropiada y permitir que las operaciones sean llevadas a cabo desde una sola consola.

La utilidad del NMS es evidente sobre todo en redes grandes, como las WAN públicas de redes corporativas. Sin un él, dichas redes requerirían la presencia constante de profesionales en mantenimiento y soporte altamente calificados en cada edificio de la ciudad donde estuviera instalado equipo de red. Por lo tanto, es necesario tener un gran número de especialistas en soporte en el departamento.

Existen múltiples problemas sin resolver en el campo de los sistemas de administración de red. Se necesitan herramientas multiprotocolo, compactas y apropiadas para la administración de la red. La mayoría de las herramientas existentes en realidad no son para la administración de redes; éstas solamente llevan a cabo la supervisión de la red y reportan eventos importantes, como fallas en los dispositivos.

6.6.3 Compatibilidad

La **compatibilidad** o las **capacidades de integración** significan que la red es capaz de incluir diferentes tipos de software y hardware (es decir, sistemas operativos disímiles que soporten pilas de protocolos diferentes, así como productos de hardware y software distintos de diversos proveedores, que puedan coexistir en la red). La red que incluye dichos elementos disímiles se llama **red heterogénea**. Si una red heterogénea opera en forma regular, se denomina **red integrada**. El método principal para construir redes integradas implica usar módulos de red diseñados de acuerdo con estándares abiertos y especificaciones.

RESUMEN

- El requerimiento principal de las redes de computadoras es garantizar una alta calidad del servicio (QoS). Cuando se utiliza este término en un sentido amplio, el concepto de QoS incluye todas las propiedades posibles de la red y sus servicios, que son deseables al usuario.
- Los requerimientos para la calidad de los servicios de red se expresan mediante el uso de valores de las características formalizadas.
- La calidad de los servicios de transporte se evalúa mediante el empleo de los siguientes grupos de características:
  - Desempeño.
  - Confiabilidad.
  - Seguridad.
  - Características únicas del proveedor, entre las que se incluyen la extensibilidad, la escalabilidad, la administración y la compatibilidad.
- El desempeño de la red se evalúa a través del uso de los dos tipos siguientes de características estadísticas: *características de velocidad de la información* y *características de retardo de la transmisión*. El primer grupo incluye la velocidad sostenida y la velocidad máxima durante los periodos de ráfaga, así como la longitud de dicho periodo. En el segundo grupo se incluyen el valor del retardo promedio, el valor promedio de la variación del retardo (*jitter*), el coeficiente de variación y los valores máximos del retardo y su variación.

- Para evaluar la confiabilidad de la red se utilizan diferentes características, incluido el *porcentaje de pérdida de paquetes;* el *coeficiente de disponibilidad*, que significa el tiempo durante el cual el sistema se puede usar, y la *tolerancia a fallas,* o la habilidad del sistema para seguir trabajando a pesar de que algunos de sus componentes fallen.
- La confiabilidad de los servicios de transporte proporcionados por la red está garantizada por la confiabilidad de sus componentes (enlaces de comunicaciones y equipo de comunicaciones), la disponibilidad de rutas alternas y la retransmisión de paquetes dañados.
- Entre las herramientas de seguridad de las redes se incluyen:
  - Herramientas para la seguridad de computadoras para proteger los recursos de información internos ubicados dentro de la LAN o en computadoras individuales.
  - Herramientas para la seguridad de las redes con el fin de proteger la información en el curso de su transmisión a través de la red.
- Las características principales de la seguridad de la información son:
  - *Confidencialidad:* garantiza que los datos estarán disponibles solamente para usuarios autorizados que tengan el derecho a acceder a esta información.
  - *Disponibilidad:* garantiza que los usuarios autorizados puedan siempre acceder a los datos.
  - *Integridad*: garantiza que los datos conserven los valores correctos, lo cual se asegura al evitar que los usuarios no autorizados puedan tener acceso a los datos, los modifiquen, eliminen o generen otros nuevos.
- Para proteger la información de la red, se utilizan los mecanismos de encriptado, autenticación, autorización y auditoría. Para transmitir datos a través de la red se utilizan técnicas de canales protegidos.

PREGUNTAS DE REPASO

1. ¿Cuál es la diferencia entre una característica y un requerimiento?
2. ¿Qué características están incluidas en el concepto de calidad del servicio (QoS) en un sentido amplio?
3. ¿Qué características del QoS son de interés para los usuarios finales solamente?, ¿cuáles interesan sólo para los proveedores y cuáles a ambos?
4. ¿Cuáles son las características del QoS, en el sentido restringido del término?
5. ¿Qué características de funcionamiento son de interés solamente para los proveedores de servicios?
6. ¿Qué instancias firman los acuerdos de nivel del servicio?
7. Sugiera un conjunto de características que quisiera incluir en el SLA, siempre y cuando usted necesite transmitir el tráfico de una aplicación de telefonía IP a través de la red.
8. ¿Qué tipo de representación de la información se usa en los resultados que se obtienen al medir retardos de paquetes?
9. ¿Cuál es la ventaja de usar características como el coeficiente de variación sobre el *jitter*?
10. ¿Qué componente no se tiene en cuenta cuando se define el tiempo del viaje redondo?
11. ¿Es posible transmitir tráfico con retardos largos pero sin *jitter*?
12. Haga una lista de los parámetros de las ráfagas. ¿Son éstos independientes?
13. ¿La velocidad de flujo promedio de los paquetes depende del retardo?

14. ¿Qué característica de la confiabilidad del servicio de transporte se utiliza en el rango a corto plazo y cuál a mediano plazo?
15. Describa los dos métodos principales para garantizar la confiabilidad de la red.
16. ¿Cuántos métodos de uso de rutas alternas están disponibles para mejorar la confiabilidad de la transmisión de tráfico?, ¿cuáles son sus ventajas y desventajas?
17. ¿Cuáles son dos componentes de la seguridad de la información?
18. ¿Cuál es la diferencia entre escalabilidad y extensibilidad?

PROBLEMAS

1. Dos switches están conectados mediante dos enlaces físicos con el fin de mejorar la confiabilidad (figura 6.7). Evalúe el volumen de datos perdidos en caso de una falla en el enlace para dos variantes de uso de estos enlaces como rutas alternas de acuerdo con el método 2, "La red encuentra dos rutas con antelación y las usa" y según el método 3, "La red halla dos rutas con antelación, pero utiliza solamente una". La longitud de cada enlace es de 5 000 km, la velocidad de transmisión de datos es de 155 Mbps y la velocidad de propagación de la señal en el enlace es de 200 000 km/seg. En ambos casos, el switch S2 detecta la falla en el enlace y conmuta al enlace de respaldo en un tiempo de 10 ms.
2. Evalúe el coeficiente de utilización del enlace si los datos son transmitidos a través de él utilizando el protocolo basado en el algoritmo del origen libre. La velocidad de transmisión es igual a 100 Mbps, el tiempo del viaje redondo (RTT) es 10 ms y los paquetes no sufren daño ni pérdida. El tamaño de los paquetes es constante e igual a 1 500 bytes, en tanto que el tamaño del reconocimiento puede despreciarse.
3. Determine el tamaño mínimo de la ventana que permita la transmisión de paquetes utilizando el enlace sin que el origen trabaje libre. La velocidad de transmisión es de 100 Mbps, el tiempo RTT es de 10 ms y el paquete no sufre daño ni se pierde. El tamaño de los paquetes es constante e igual a 1 500 bytes, mientras que el tamaño del reconocimiento puede despreciarse.



FIGURA 6.7 Rutas alternas.

7

MÉTODOS PARA ASEGURAR LA CALIDAD DEL SERVICIO

DESCRIPCIÓN DEL CAPÍTULO

7.1 INTRODUCCIÓN

En la actualidad, los métodos para asegurar la calidad del servicio ocupan una de las posiciones más importantes entre las tecnologías de las redes de conmutación de paquetes, dado que la operación de las aplicaciones multimedia modernas como la telefonía IP, la difusión de video y radio y el aprendizaje remoto interactivo es imposible sin su implementación. Dichos métodos trabajan con las características de la red de los tres grupos siguientes:

- Velocidad de información.
- Retardos de paquetes.
- Pérdidas de paquetes.

Las definiciones de estas características se proporcionaron en el capítulo anterior.

La técnica QoS se enfoca en la influencia que tienen los dispositivos de comunicaciones en la transmisión de tráfico. Los métodos QoS utilizan diferentes algoritmos para la administración de colas, para la reservación y para la retroalimentación, que permiten reducir los efectos negativos a un valor mínimo aceptable por el usuario.

Las colas son atributos genéricos de las redes de conmutación de paquetes. El principio de conmutación de paquetes en sí mismo supone la presencia de memorias en cada entrada o interfaz de salida del switch de paquetes. El almacenamiento de paquetes durante tiempos de congestión de la red representa el mecanismo principal para soportar el tráfico en ráfagas, asegurando un alto desempeño en este tipo de redes. Por otro lado, las colas significan retardos indefinidos y variables en la transmisión de paquetes a lo largo de toda la red, la fuente principal de problemas del tráfico que es sensible al retardo. Como los prestadores de servicios de redes de paquetes tienen un gran interés en la transmisión de dicho tráfico, éstos requieren herramientas especiales diseñadas con el fin de asegurar el compromiso entre su intención de cargar su red al máximo y su deseo de cumplir con los requerimientos de QoS para todos los tipos de tráfico de red.

Todas estas características describen los efectos negativos de las colas. En la actualidad, si se presenta congestión en las redes, esto generalmente reduce la velocidad de flujo durante los periodos de congestión, así como también los retardos de paquetes y aun su pérdida. Los paquetes se pierden cuando la cola satura totalmente las memorias.

Los métodos de QoS utilizan varios mecanismos para reducir los efectos negativos de las colas. El conjunto de estos mecanismos es muy grande y éstos se estudiarán con el suficiente detalle. La mayoría de ellos tienen en cuenta los diferentes tipos de tráfico que existen en la red.

Los métodos de QoS pueden complementarse mediante métodos de ingeniería de tráfico, que administren las rutas de tráfico para equilibrar las cargas y eliminar la saturación de las colas.

7.2 APLICACIONES Y QoS

PALABRAS CLAVE: tipos de aplicaciones, requerimientos de QoS, velocidad de bits, retardos de paquetes, daños o pérdidas, aplicaciones asíncronas, aplicaciones interactivas, aplicaciones isócronas, aplicaciones hipersensibles a los retardos, sensibilidad de la aplicación a los retardos de paquetes y clasificación de las aplicaciones de ATM.

7.2.1 Requerimientos de diversos tipos de aplicaciones

La tendencia actual de la convergencia de los diferentes tipos de redes descritas en el capítulo 1 significa que la red de datos tiene que transportar todo tipo de tráfico y no solamente el de acceso a archivos y el de correo electrónico.

En la sección anterior se hizo una lista de las diferentes características de QoS que se utilizan para evaluar la calidad de transmisión de tráfico a través de la red. Dichas características son especialmente importantes cuando la red transmite de forma simultánea los distintos tipos de tráfico, por ejemplo: el tráfico de las aplicaciones web y el tráfico de voz. Esto se debe a que cada tipo de tráfico tiene diferentes requerimientos en las características del QoS. La tarea que implica lograr la observancia simultánea de *todos* los requerimientos del QoS de *todos* los tipos de tráfico es muy difícil. Por lo tanto, se suele seleccionar el siguiente método: todos los tipos de tráfico existente en la red se categorizan en varias clases de tráfico agregado y después se hace todo esfuerzo para lograr la observancia simultánea de los requerimientos de QoS para cada una de estas clases de tráfico.

Se ha llevado a cabo una enorme cantidad de investigación con el fin de clasificar las aplicaciones por tráfico generado. Las siguientes características de la aplicación se tomaron como el criterio principal de tráfico:

- La predictibilidad relativa de la velocidad de la información del tráfico generado por una aplicación.
- La sensibilidad de las aplicaciones a los retardos de los paquetes.
- La sensibilidad de las aplicaciones al daño o pérdida de paquetes.

7.2.2 Predictibilidad de la velocidad de información

En relación con la predictibilidad de la velocidad de la información, todas las aplicaciones se dividen en: las que generan tráfico regular y aquellas que generan tráfico en ráfagas.

Las aplicaciones que generan tráfico regular producen datos a una **velocidad constante** (CBR). Si se utiliza la conmutación de paquetes, el tráfico de dichas aplicaciones será una secuencia de paquetes del mismo tamaño, igual a B bits, que se suceden uno tras otro después del mismo espacio de tiempo T (figura 7.1).

La velocidad constante del tráfico regular (CBR) puede calcularse mediante el promedio de un periodo T:

$$\text{CBR} = B/T \text{ (bps)} \tag{7.1}$$

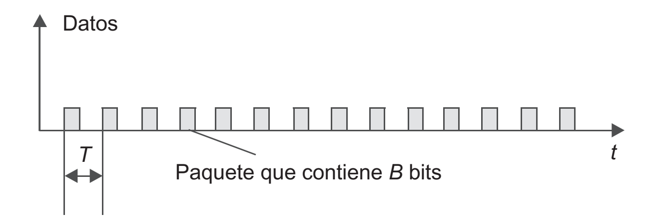


FIGURA 7.1 Tráfico de flujos.

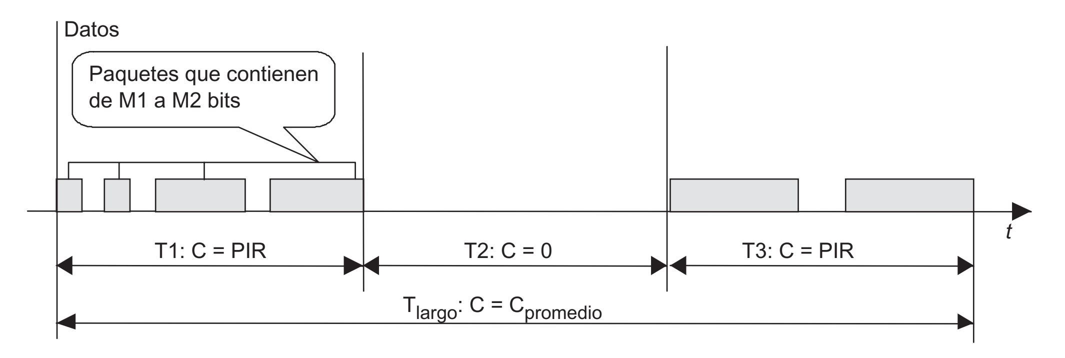


FIGURA 7.2 Tráfico de ráfagas.

Dicha velocidad es menor que la velocidad de bits máxima nominal del protocolo de transmisión de datos, ya que existen pausas entre paquetes. Como se estudiará en el capítulo 12, la máxima velocidad de transmisión que utiliza el protocolo Ethernet es de 9.76 Mbps (cuando la trama tiene una longitud máxima), más pequeña que la velocidad nominal de este protocolo (10 Mbps).

Las aplicaciones que generan tráfico en ráfagas están caracterizadas por niveles de predictibilidad bajos, ya que los periodos de silencio se hallan seguidos de ráfagas durante las cuales los paquetes se siguen entre sí de una manera muy densa. Como resultado, el tráfico tiene una **velocidad de bits variable** (*VBR*), como se muestra en la figura 7.2. Por ende, cuando se trabaja con aplicaciones de servicio de archivos, la intensidad del tráfico generado por dichas aplicaciones podría disminuir a cero (siempre y cuando no se transmitan archivos) o incrementarse al máximo (limitado solamente por las características funcionales de la red) cuando el servidor de archivos transmita un archivo.

La figura 7.2 muestra tres periodos de medida: $T1$, $T2$ y $T3$. Para simplificar los cálculos, se asume que las velocidades pico durante el primer y tercer periodos son iguales y tienen el valor del PIR y que ambos periodos tienen la misma duración T. Dado el valor T, es posible calcular el tamaño de la ráfaga, B, el cual es igual al número de bits transmitidos durante el periodo de ráfaga:

$$B = PIR \times T \tag{7.2}$$

Por lo tanto, el tamaño de ráfaga de los periodos $T1$ y $T3$ es igual a B, y para el periodo $T2$ es igual a cero.

En este ejemplo, es posible calcular el coeficiente de ráfaga. Recuerde que éste es igual al cociente de la velocidad pico en algún espacio de tiempo y la velocidad de tráfico promedio medida durante un periodo prolongado. La velocidad pico de los periodos $T1$ y $T3$ es igual a B/T y la velocidad promedio durante el periodo de medida completo $C_{promedio} = T1 + T2 + T3$ es igual a $2B/3T$. De aquí que el coeficiente de ráfaga es igual a $3/2 = 1.5$.

7.2.3 Sensibilidad de la aplicación a los retardos de los paquetes

Otro criterio para clasificar la aplicación por tipo de tráfico es la sensibilidad de la aplicación a los retardos de los paquetes y sus variantes. Los principales tipos de aplicaciones, en orden creciente respecto a la sensibilidad a los retardos de los paquetes, se mencionan a continuación:

- **Aplicaciones asíncronas**. Con este tipo de aplicación, prácticamente no existen limitaciones al tiempo de retardo de paquetes. En este caso, los usuarios trabajan con **tráfico elástico**. El correo electrónico es un ejemplo típico de dicha aplicación.
- **Aplicaciones interactivas**. Los usuarios pueden observar la presencia de retardos; sin embargo, éstos no tienen efectos negativos en la funcionalidad de la aplicación. Un editor de textos que se utilice para acceder a archivos remotos es un ejemplo de dicha aplicación.
- **Aplicaciones isócronas**. Éstas tienen un umbral de sensibilidad a las variaciones del retardo. Si se excede dicho valor, la funcionalidad de la aplicación se degradará de manera drástica. Por ejemplo, cuando se trabaja con aplicaciones de transmisión de voz, la calidad de la reproducción de la voz se degrada de manera significativa después de que se ha excedido el valor de umbral de la variación de retardos (100-150 mseg).
- **Aplicaciones muy sensibles a los retardos.** Los retardos en la entrega de datos prácticamente reducen a cero la funcionalidad de la aplicación. Las aplicaciones que llevan a cabo un control en tiempo real sobre los objetos técnicos representan un ejemplo de dichas aplicaciones. Si la señal controladora sufre un retraso, el objeto podrá dañarse.

En general, las funciones interactivas de una aplicación siempre aumentan su sensibilidad a los retardos; por ejemplo, la difusión de información de audio puede tolerar retardos significativos en la entrega de paquetes (mientras permanezca sensible a las variaciones de retardos); sin embargo, el teléfono interactivo o las videoconferencias no los toleran. Lo anterior puede observarse claramente cuando la conversación es traducida mediante el uso de un satélite. Las pausas prolongadas que se presentan en la conversación suelen provocar confusión entre los participantes. En consecuencia, ambos empiezan a desesperarse y comienzan a hablar de manera simultánea.

NOTA *Junto con la clasificación que se hizo, la cual proporciona una pequeña diferencia entre la sensibilidad de la aplicación a los retardos y sus variaciones, existe otra clasificación que ofrece una división más burda de las aplicaciones usando el mismo criterio. De acuerdo con esta segunda clasificación, existen dos tipos de aplicaciones —asíncronas con tráfico elástico y síncronas con tráfico sensible al retardo (o sensible al tiempo)—. Las* ***aplicaciones asíncronas*** *son aquellas que toleran retardos en la entrega de datos de hasta varios segundos. Las demás, cuya funcionalidad sufre retardos en la entrega de datos, se clasifican como* ***aplicaciones sincrónicas.*** *A su vez, las aplicaciones interactivas pueden clasificarse como asíncronas (por ejemplo, editores de texto) o sincrónicas (por ejemplo, el software para videoconferencia).*

7.2.4 Sensibilidad de la aplicación a las pérdidas de los paquetes

El último criterio para clasificar las aplicaciones es su sensibilidad a las pérdidas de paquetes. Como regla general, las aplicaciones se dividen en dos grupos.

- **Aplicaciones sensibles a las pérdidas**. Prácticamente todas las aplicaciones que transmiten datos alfanuméricos (documentos de textos, código fuente, arreglos numéricos, etc.) son muy sensibles a la pérdida de fragmentos de datos, sin importar qué tan pequeños sean éstos. A menudo, dichas pérdidas hacen que toda la información recibida con éxito sea prácticamente inútil. Por ejemplo, un solo byte que se pierda en el código fuente de un programa puede hacerlo totalmente inútil. Todas las aplicaciones de red convencionales (servicios de archivos, sistemas de administración de bases de datos, servicio de correo electrónico, etc.) pertenecen a este grupo.

- **Aplicaciones tolerantes a la pérdida de datos**. En este grupo se incluyen muchas aplicaciones que transmiten el tráfico al transportar información mediante procesos físicos inerciales. La tolerancia a las pérdidas significa que una pequeña cantidad de datos perdidos puede ser recuperada con base en la información recibida con éxito. Por lo tanto, si un solo paquete que transporta varias mediciones secuenciales de voz llegara a perderse durante la reproducción, los datos faltantes podrían recuperarse mediante aproximaciones con base en los valores adyacentes. En este grupo de aplicaciones se incluyen la mayoría de las que trabajan con tráfico multimedia (aplicaciones de audio y video). No obstante, el nivel de tolerancia a las pérdidas tiene sus límites y el porcentaje de pérdida de paquetes no puede ser demasiado elevado (como regla general, no es mayor a 1%).

No todo el tráfico multimedia tolera las pérdidas de datos; por ejemplo, la voz y el video comprimido son muy sensibles a las pérdidas; en consecuencia, se clasifican como aplicaciones del primer tipo.

7.2.5 Clases de aplicaciones

Una aplicación puede pertenecer a diferentes grupos según el criterio de clasificación que se utilice —predicción relativa de la velocidad de datos, sensibilidad del tráfico a los retardos de paquetes y sensibilidad del tráfico a las pérdidas y daños de paquetes—. Esto significa que las aplicaciones regulares pueden clasificarse en sincrónicas y asíncronas. Una aplicación sincrónica puede ser sensible a la pérdida de paquetes o puede tolerarlas. Sin embargo, en la práctica se ha observado que entre las combinaciones de rasgos de las aplicaciones, algunas de esas combinaciones son características de la mayoría de las aplicaciones que se utilizan en la actualidad.

Por ejemplo, una aplicación caracterizada como "generadora de tráfico regular, isócrono, tolerante a retardos de datos" corresponde a aplicaciones muy conocidas, como telefonía IP, soporte a videoconferencia y difusión de audio a través de Internet. Por otro lado, existen combinaciones de estas características para las que es muy difícil proporcionar un ejemplo de una aplicación existente. Una combinación podría ser "generador de tráfico regular, asíncrono y sensible a las pérdidas".

No son muy numerosas las combinaciones estables de las características correspondientes a clases específicas de aplicaciones populares. Por ejemplo, durante la estandarización de la tecnología ATM, que originalmente se diseñó para soportar varios tipos de tráfico, se definieron las cuatro **clases de aplicaciones**: A, B, C y D. En cada una de éstas se recomienda utilizar un conjunto específico de características QoS; además, para todas las aplicaciones que no coincidan con estas clases, se definió una clase especial (clase X), para la cual la combinación de las características de la aplicación puede ser arbitraria.

La clasificación ATM es, por el momento, la más detallada y generalizada; no depende de la tecnología, ni requiere que la conozcamos y puede verse de manera resumida en la tabla 7.1.

Esta clasificación de las aplicaciones sirve como base para definir los requerimientos típicos de los parámetros QoS y los mecanismos utilizados en las redes actuales.

7.3 ANÁLISIS DE COLAS

PALABRAS CLAVE: cola, teoría de colas, modelo M/M/1, flujo de solicitud, servidor, memoria, FIFO, longitud de la cola, tiempo de espera, proceso aleatorio, coeficiente de utilización y coeficiente de variación.

TABLA 7.1 Clases de tráfico

Clases de tráfico	Características
A	Velocidad de bits constante (CBR) Sensible a los retardos Orientado a la conexión Ejemplos: tráfico de voz y de televisión Características del QoS: velocidad pico de información, retardo y *jitter*
B	Velocidad de bits variable (VBR) Sensible a los retardos Orientado a la conexión Ejemplos: voz comprimida, video comprimido Parámetros QoS: velocidad pico de información, ráfaga, velocidad sostenida de información, retardo y *jitter*
C	Velocidad de bits variable (VBR) Tráfico elástico Orientado a la conexión Ejemplos: tráfico de las redes de computadoras, en el que los nodos terminales trabajan utilizando protocolos orientados a la conexión (Frame Relay, X.25 y TCP) Parámetros QoS: velocidad pico de información, ráfaga, y velocidad sostenida de información
D	Velocidad de bits variable (CBR) Tráfico elástico Sin conexión Ejemplos: tráfico en las redes de computadoras, en el que los nodos terminales trabajan utilizando los protocolos sin conexión (IP/UDP y Ethernet) Parámetros QoS: no definidos
X	Tipo de tráfico definido por el usuario y sus parámetros

Si usted definió las características principales QoS y ha formulado sus requerimientos, habrá resuelto la mitad del problema. El usuario formula los requerimientos del QoS mediante el empleo de un conjunto de valores de umbral de las características del QoS. Por ejemplo, el usuario puede especificar que la varianza del retardo de los paquetes no deba exceder de 50 mseg con una probabilidad de 0.99.

No obstante, ¿cómo puede el usuario asegurarse de que la red es capaz de llevar a cabo de manera exitosa la tarea formulada?, ¿qué pasos deben llevarse a cabo para garantizar que las variaciones de los retardos no excedan el valor especificado?, ¿cómo puede garantizar el usuario que la velocidad promedio del flujo de salida corresponda a la velocidad promedio del flujo de entrada?

Durante mucho tiempo, estas preguntas no se consideraron de gran importancia. Las redes de conmutación de paquetes se diseñaron originalmente para la transmisión de tráfico asíncrono; por lo tanto, los retardos podían tolerarse. No obstante, en la actualidad, cuando las redes de datos comenzaron a transportar diferentes tipos de tráfico (incluido el tráfico en tiempo real), los aspectos del QoS se volvieron urgentes.

Para comprender los mecanismos de soporte del QoS, es necesario investigar primero el proceso de colas en los dispositivos de red y comprender los factores más importantes que influyen en la longitud de las colas.

7.3.1 Modelo M/M/1

La teoría de colas es una rama de las matemáticas aplicadas que estudia los procesos de colas. No vamos a profundizar en el estudio de los fundamentos matemáticos de esta teoría, sino que el enfoque estará en analizar algunas de sus conclusiones, las cuales son básicas para examinar el problema de QoS.

La figura 7.3 muestra el modelo más simple de la teoría de colas, conocido como modelo M/M/1.[1]

Los elementos principales de este modelo se relacionan a continuación:

- Flujo de entrada de las solicitudes abstractas de servicio.
- Memoria.
- Flujo de salida de las solicitudes atendidas.
- Servidor.

Las solicitudes llegan a la entrada de la memoria en instantes aleatorios. Si la memoria está vacía y el servidor se halla libre cuando llegue una nueva solicitud, ésta se enviará de inmediato al servidor. El tiempo de atención también es aleatorio.

Si cuando llega una solicitud, la memoria está vacía pero el servidor está ocupado atendiendo la solicitud anterior, la solicitud que llegó deberá esperar en la memoria hasta que el servidor se encuentre disponible. En cuanto el servidor termine de atender la solicitud anterior, la nueva solicitud se transferirá a la salida y el servidor recuperará la solicitud siguiente de la memoria. Las solicitudes que abandonan el servidor constituyen el flujo de salida; a su vez, la memoria es infinita, lo cual significa que las solicitudes nunca se pierden debido a una saturación de la memoria.

Si la solicitud que acaba de llegar encuentra que la memoria está vacía, se colocará en la cola y esperará a ser atendida. Las solicitudes son recuperadas de la cola de acuerdo con el orden en el que llegaron —es decir, según el criterio de servicio, **Primera que entra, primera que sale** (**FIFO**).

La teoría de colas permite evaluar una longitud de cola promedio y un tiempo de espera promedio para este modelo, en función de las características del flujo de entrada y el tiempo de servicio.

Suponga que el tiempo promedio entre las llegadas de dos solicitudes es igual a T. Esto significa que la velocidad de las llegadas de solicitudes, tradicionalmente designadas con la letra λ en la teoría de colas, es:

[1] Aquí 1 significa que el modelo tiene un servidor y la primera M significa el tipo de función de distribución para los intervalos de llegada de las solicitudes (markoviana), mientras que la segunda M designa el tipo de distribución de los tiempos de atención (también markoviana).

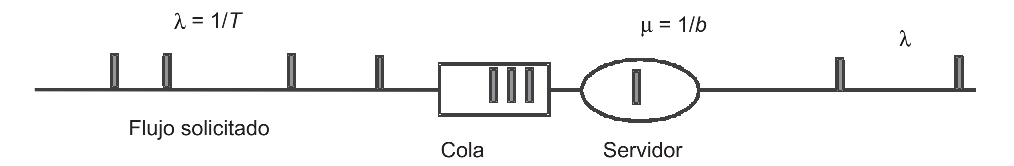


FIGURA 7.3 Modelo M/M/1.

$$\lambda = 1/T \text{ solicitudes por segundo} \quad (7.3)$$

El proceso aleatorio de las llegadas de solicitudes en este modelo se describe mediante la función de distribución de los intervalos entre las llegadas de solicitudes. Para efectos de simplicidad y obtención de resultados analíticos compactos, se asume en general que estos intervalos se hallan descritos mediante la famosa distribución **markoviana** (también conocida como de **Poisson**), cuya densidad de distribución se muestra en la figura 7.4. A partir de esta ilustración, es evidente que el flujo de entrada es totalmente en ráfagas, pues existen probabilidades diferentes de cero en el intervalo entre solicitudes que son muy pequeñas (cercanas a cero) o muy largas. La desviación promedio de los intervalos también es igual a T; por lo tanto, la desviación estándar es $T/T = 1$.

Asimismo, suponga que el tiempo de servicio promedio de una sola solicitud es igual a b. Esto significa que el servidor es capaz de enviar solicitudes a la salida a una velocidad de $1/b = \mu$. Una vez más, para obtener resultados compactos en forma analítica, se supone que el tiempo de servicio es una variable aleatoria caracterizada por la densidad de la distribución de Poisson.

Con base en estas suposiciones, podemos obtener un resultado simple para el tiempo promedio que deben esperar las solicitudes en la cola:

$$W = \rho \times b/(1 - \rho) \quad (7.4)$$

Aquí, ρ denota la relación $\lambda:\mu$.

El parámetro r es el **coeficiente de utilización** del servidor. En cualquier periodo, este coeficiente es igual a la relación entre el tiempo que está ocupado el servidor y el tiempo total de todo el periodo.

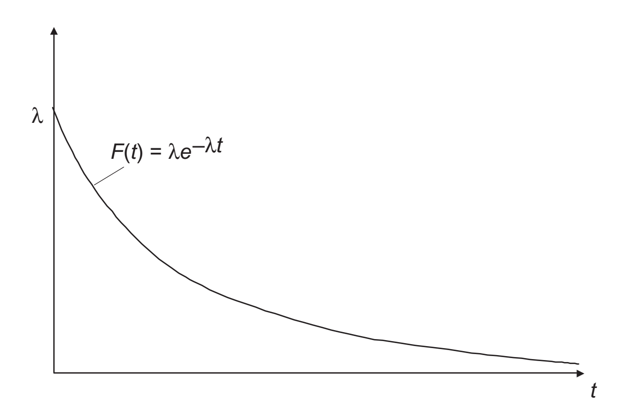


FIGURA 7.4 Densidad de la distribución del flujo de entrada.

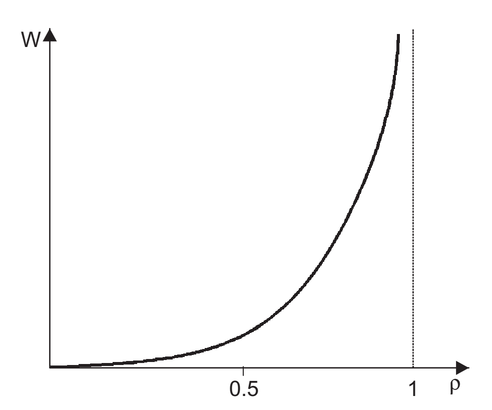


FIGURA 7.5 Dependencia del tiempo de espera promedio de las solicitudes con respecto a ρ.

La dependencia del tiempo de espera promedio *W* respecto a ρ se muestra en la figura 7.5. Como puede observarse claramente, el parámetro ρ desempeña un papel fundamental en el proceso de la cola. Si el valor de ρ es cercano a cero, el tiempo de espera promedio también es cercano a cero. Esto significa que las solicitudes no tienen que esperar en la memoria (está vacía en el momento en que éstas llegan); las solicitudes se dirigen inmediatamente al servidor. Sin embargo, si ρ tiende a 1, el tiempo de espera aumentará de manera muy rápida y la dependencia será de una naturaleza no lineal. Dicho comportamiento de la cola es intuitivamente claro, ya que ρ representa el cociente de la velocidad promedio del flujo de entrada y la velocidad promedio a la que es atendido. A medida que los valores promedio de los intervalos entre paquetes están más cercanos al tiempo de servicio promedio, es más difícil que el servidor maneje la carga.

7.3.2 M/M/1 como un modelo para el procesamiento de paquetes

La figura 7.6 muestra la correspondencia entre los elementos del modelo descrito anteriormente y los elementos de la red de conmutación de paquetes:

- El flujo de los paquetes que llegan a la entrada de la interfaz del switch corresponde al flujo de entrada de las solicitudes de servicio. El parámetro 1 corresponde a la velocidad de llegada de paquetes.
- La memoria de la interfaz de entrada del switch corresponde a la memoria del modelo M/M/1.
- El procesador que maneja los paquetes y los envía a la interfaz de salida corresponde al servidor. El tiempo promedio de envío de paquetes desde la memoria de entrada al canal de salida corresponde al tiempo promedio entre la solicitud y el servicio. El parámetro m corresponde al desempeño del recurso (el procesador o la interfaz de un switch).

Es necesario mencionar que el modelo descrito con anterioridad presenta una descripción muy simplificada de los procesos que se llevan a cabo en la red. Este modelo no tiene en cuenta muchas de las características típicas del procesamiento de paquetes (el tamaño finito de la memoria del switch, el tiempo distinto de cero que se requiere para cargar el paquete en la memoria, etc.). Sin embargo, su valor reside en que demuestra la naturaleza cualitativa del comportamiento de la cola; por lo tanto, resulta útil para comprender los factores principales que influyen en la longitud de la cola.

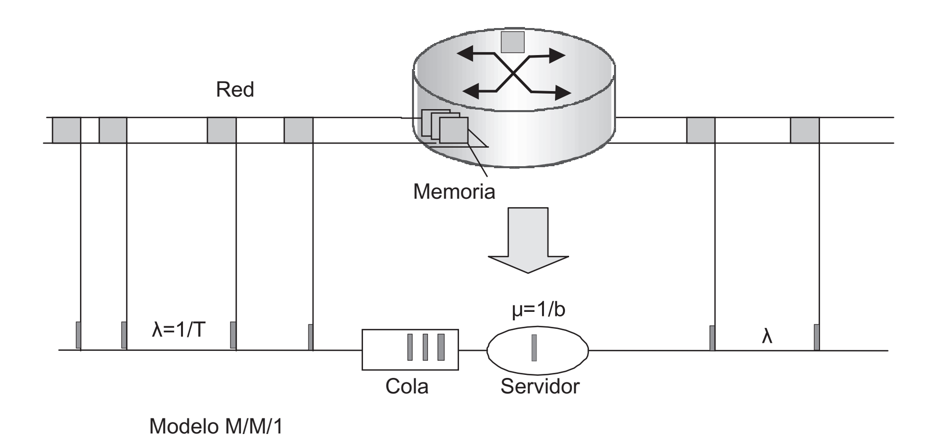


FIGURA 7.6 Correspondencia del modelo M/M/1 con los elementos de la red.

Los ingenieros de redes están muy familiarizados con la gráfica que se muestra en la figura 7.5 y la interpretan como la dependencia que tienen los retardos de la red en la carga de ésta. El parámetro ρ del modelo descrito anteriormente corresponde al coeficiente de utilización del recurso de red que participa en la transmisión del tráfico. Algunos ejemplos son la interfaz del switch, el procesador del switch, el canal y el medio compartido.

La figura 7.5 también muestra algo inesperado. Resulta difícil imaginar que el servidor o el recurso de red prácticamente deje de manejar la carga cuando su coeficiente de utilización es cercano a 1. Después de todo, en este caso, la carga no excede sus capacidades; por el contrario, solamente tiende hacia este límite. Asimismo, las razones que explicarían la existencia de las colas en los valores de ρ alrededor de 0.5 no son intuitivas. Las capacidades de transmisión de tráfico exceden la carga dos veces, pero las colas existen y, en promedio, la cola contiene varias solicitudes en espera (paquetes).

Estos resultados aparentemente paradójicos son característicos de los sistemas en los que se llevan a cabo procesos aleatorios. Como λ y μ son velocidades promedio en espacios de tiempo largos, nada evita que los flujos se alejen de estos valores por periodos cortos. La cola se genera cuando la velocidad de la llegada de paquetes excede de manera significativa la velocidad de servicio.

> La conclusión principal a la que puede llegarse a partir de este modelo es la siguiente: para lograr un alto QoS, es necesario evitar que el coeficiente de utilización de los recursos de la red se eleve a un valor mayor que 0.9.

La sobrecarga de recursos puede dar como resultado la degradación total de la red. Si esto sucede, la velocidad efectiva de transmisión de datos puede ser cero, a pesar de que la red continúe transmitiendo paquetes. Éste sería el caso si los retardos en la entrega de todos los paquetes excedieran cierto valor de umbral. Como resultado, el nodo de destino elimina dichos paquetes debido a que el tiempo ha sido excedido. Si los protocolos que operan en la red utilizaran procedimientos confiables de transmisión de datos, basados en reconocimientos y retransmisión de paquetes, el proceso de congestión crecería como una avalancha.

Existe otro parámetro importante que ejerce una influencia directa en el proceso de colas en las redes de conmutación de paquetes. Se trata de una variación de los intervalos entre paquetes del flujo de paquetes de salida (es decir, la ráfaga del tráfico entrante). Hemos

analizado el comportamiento del modelo M/M/1 con base en la suposición de que el flujo de entrada queda descrito mediante la distribución de Poisson. Dicha distribución tiene una desviación estándar muy significativa del retardo (recuerde que la variación promedio es igual a *T*, siempre y cuando el intervalo promedio sea igual a *T* y el coeficiente de la varianza sea 1). ¿Qué pasará si la variación de los intervalos entre paquetes del flujo de salida es más pequeña? o ¿cuál será el efecto si el flujo de entrada es en ráfagas (o sea, la desviación estándar es 10 o incluso 100)?

Por degracia, los modelos de la teoría de colas no proporcionan dependencias analíticas sencillas similares a la fórmula 7.4 para este caso. Por lo tanto, para obtener los resultados, el usuario tiene que emplear métodos de simulación de redes o llevar a cabo mediciones en una red práctica.

La figura 7.7 muestra la familia de curvas generadas mediante un modelo de simulación y corresponde a la dependencia de *W* en ρ, obtenida para distintos valores del coeficiente de variación (*CV*) del flujo de entrada. El modelo de simulación tuvo en cuenta la existencia de un retardo constante en una red práctica. Una de las curvas con el parámetro *CV* igual a 1 corresponde al flujo de entrada poissoniano. A partir de la ilustración, se puede observar que a medida que es menor la ráfaga del flujo de entrada (*CV* tiende a cero), también es menor el efecto del proceso en forma de avalancha de la generación de colas cuando el coeficiente de utilización se acerca al valor 1. Por otro lado, a medida que el valor de *CV* es mayor, este proceso comenzará a manifestarse por sí solo antes (y a valores menores que ρ).

Se puede llegar a dos conclusiones a partir del análisis de las gráficas que se muestran en la figura 7.7.

- La información acerca del uso de recursos por sí sola (ρ) no es suficiente para determinar los retardos en las colas de los switches de la red. Para obtener una evaluación más precisa, es necesario conocer los parámetros de las ráfagas de tráfico.
- Para mejorar el QoS (reducir el nivel de retardo), es necesario tratar de emparejar el tráfico (o sea, reducir el número de ráfagas).

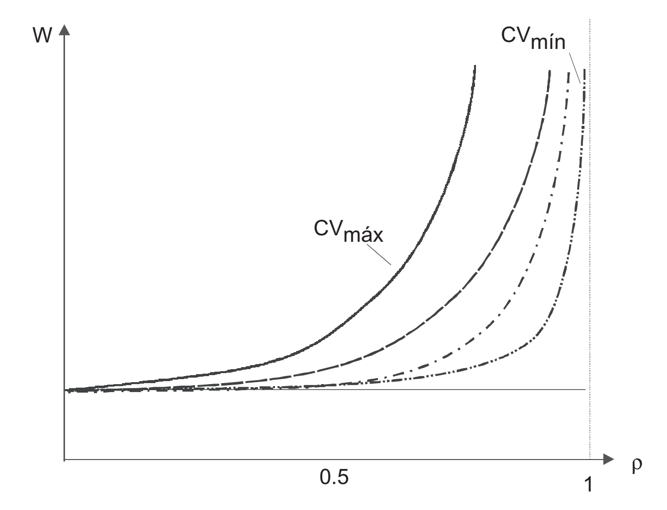


FIGURA 7.7 Influencia de las ráfagas de tráfico en los retardos.

7.4 MECANISMOS DE QoS

PALABRAS CLAVE: requerimientos del QoS, mecanismos del QoS, coeficiente de utilización, modo con baja carga, red con demasiada carga, tráfico sensible al retardo, tráfico en tiempo real, tráfico sincrónico, tráfico elástico y tráfico asíncrono.

7.4.1 Operación en modo de baja carga

En general, un gran número de flujos de información viajan a través de la red de manera simultánea. Cada uno de ellos necesita servicios de acuerdo con requerimientos específicos de QoS. Cada uno de dichos flujos circula a través de varios switches a lo largo de su ruta desde el nodo de origen hasta el nodo de destino. En cada switch pasa a través de dos colas: hacia el procesador del switch y hacia la interfaz de salida del mismo. Usted ya ha investigado que el factor más importante que ejerce una influencia directa en los valores del retardo y, por ende, en el QoS de la red, es el coeficiente de utilización de recursos. Por lo tanto, para asegurar el QoS requerido, es importante asegurar que el coeficiente de utilización de cada recurso (los procesadores y las interfaces de los switches) que sirve al flujo en su ruta no exceda el valor predefinido.

El método más simple para garantizar la observación de los requerimientos del QoS de todos los flujos consiste en operar la red en modo de baja carga cuando todos los procesadores e interfaces de los switches utilizan solamente de 20% a 30% de su capacidad máxima.

Sin embargo, lo anterior neutraliza la ventaja principal de la red de conmutación de paquetes, la cual es su alto desempeño cuando transmite tráfico en ráfagas.

7.4.2 Diferentes clases de servicio

Soportar el QoS en una red con un **alto volumen de tráfico** representa una tarea compleja pero importante. En este caso, la existencia de diferentes clases de flujos dentro de la red es de gran ayuda. Para efectos de simplicidad, divida todos los flujos en dos clases:

- **Tráfico sensible al retardo** (tráfico en tiempo real o sincrónico).
- **Tráfico elástico** que puede tolerar retardos significativos, pero aún es sensible a las pérdidas de datos (tráfico asíncrono).

No conocemos la dependencia exacta entre los retardos y el coeficiente de utilización de los recursos, pero sí su dependencia general. Si para tráfico sensible a los retardos aseguramos un coeficiente de utilización de cada recurso no mayor que 0.2, será evidente que los retardos en cada cola resultarán muy pequeños. Estos retardos probablemente sean aceptables en la mayor parte de aplicaciones en esta clase. Para tráfico elástico, es posible permitir un coeficiente de utilización mayor (aunque no deba exceder el valor de 0.9). Para asegurarnos de que los paquetes de esta clase no se pierdan, es necesario proporcionar una capacidad de memoria suficiente para almacenar todos los paquetes que lleguen durante los periodos de ráfagas. El efecto que se logra con dicha distribución de carga se muestra en la figura 7.8.

Los retardos del tráfico sensible al retardo son iguales a $w_{S,}$ mientras que los retardos del tráfico elástico son w_e.

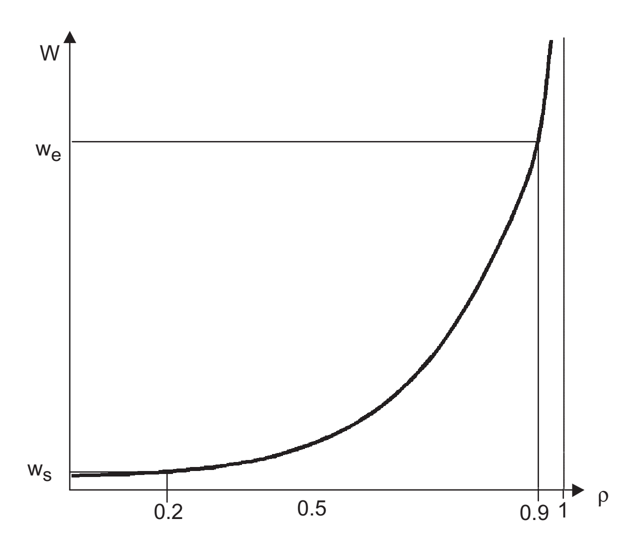


FIGURA 7.8 Atención del tráfico elástico y del tráfico en tiempo real.

Por mucho tiempo, las redes de conmutación de paquetes solamente transmitían tráfico elástico. De esta manera, los principales requerimientos del QoS incluían la minimización de pérdidas de paquetes y proporcionaban una forma de asegurar que los coeficientes de utilización de cada recurso de red no excedieran 0.9. Los métodos para resolver esta tarea se conocen como *métodos para el control de la congestión*.

A principios de la década de 1990, cuando fue necesario transmitir tráfico sensible al retardo, la situación se tornó más compleja y se requirió buscar nuevos métodos. Durante ese tiempo apareció el término *calidad de servicio*, el cual reflejaba los requerimientos más detallados y diferenciados de los diversos tipos de tráfico.

A fin de lograr distintos valores de los coeficientes de utilización de recursos para estas dos clases de tráfico, es necesario soportar dos colas en cada switch para cada recurso. El algoritmo de recuperación de paquetes de las colas debe dar preferencia a las colas de los paquetes que son sensibles a los retardos. Si todos los paquetes de esta cola se atienden en un modo prioritario y los paquetes de otra cola se atienden en este modo sólo cuando la primera cola esté vacía, la segunda cola no ejercerá influencia alguna en la primera, como si ésta no existiera. Por ende, si el cociente de la velocidad promedio del tráfico prioritario (λ_1) y el desempeño de los recursos (μ) es de 0.2, el coeficiente de utilización para este tráfico también será de 0.2.

En el caso del tráfico elástico, para los paquetes que siempre esperan hasta que los paquetes prioritarios son atendidos, el coeficiente de utilización debe calcularse de otra forma. Si la velocidad promedio de tráfico elástico es igual a λ_2, el coeficiente de utilización para este tráfico será igual a $(\lambda_1 + \lambda_2)/\mu$. Por ende, si queremos asegurarnos de que el coeficiente de utilización para el tráfico elástico sea de 0.9, su intensidad deberá calcularse de acuerdo con la fórmula siguiente: $\lambda_2/\mu = 0.7$.

La idea general que sirve como base para todos los métodos de soporte del QoS es la siguiente: el desempeño total de cada recurso debe estar *no uniformemente* distribuido entre las diversas clases de tráfico.

Es posible incluir más de dos clases de servicio y tratar de asegurar que cada una de ellas sea atendida de acuerdo con su valor del coeficiente de utilización. Cuando se resuelve esta tarea, se pueden mejorar adicionalmente las características del QoS mediante el uso de otros métodos (por ejemplo, al reducir las ráfagas de tráfico).

Ahora es necesario investigar cómo se pueden asegurar tales condiciones para las diferentes clases de tráfico en cada nodo de la red.

Los diseñadores de redes han tratado de resolver este problema al crear redes de conmutación de paquetes. Para lograr dicho propósito, se utilizan diferentes mecanismos en varias combinaciones.

7.5 MECANISMOS PARA LA ADMINISTRACIÓN DE COLAS

PALABRAS CLAVE: administración de colas, algoritmo FIFO, prioridad, algoritmos de colas con prioridad, clasificación del tráfico, política de la administración de la red, tamaño de la memoria, puntos de clasificación del tráfico, granularidad, tráfico agregado, algoritmo de colas ponderadas y colas justamente ponderadas.

La administración de colas es necesaria para la operación durante periodos de congestión, cuando los dispositivos de la red no pueden transmitir paquetes hacia la interfaz de salida a la misma velocidad que éstos llegan. Si dicha saturación es causada por un desempeño insuficiente de la unidad de procesamiento del dispositivo de red, la cola de entrada de la interfaz de entrada correspondiente se utiliza para el almacenamiento temporal de los paquetes sin procesar. Cuando se diferencian las solicitudes en varias clases, puede haber varias colas de entrada en la misma interfaz. Si la sobrecarga es causada por un ancho de banda insuficiente en la interfaz de salida, los paquetes son almacenados de manera temporal en la cola o colas de salida de esta interfaz.

7.5.1 Algoritmo FIFO

La esencia del **algoritmo FIFO** tradicional reside en que si se presenta una sobrecarga, todos los paquetes se colocan en una cola única y son recuperados de ella según el orden en el que llegaron —es decir, el primero que llegó es el primero en salir—. En todos los dispositivos de conmutación de paquetes, el algoritmo FIFO se utiliza por omisión. Sus ventajas incluyen su facilidad de implementación y el hecho de que no es necesario configurarlo. Sin embargo, tiene una gran desventaja: *la imposibilidad del procesamiento diferenciado de los paquetes que pertenezcan a flujos distintos*. Todos los paquetes se colocan en la cola común y tienen la misma prioridad. Esto se relaciona con los paquetes de tráfico de voz sensible al retardo, así como con los paquetes de tráfico de respaldo, los cuales son insensibles a los retardos pero resultan muy intensos y sus ráfagas prolongadas son capaces de retardar el tráfico de voz por un tiempo muy largo.

7.5.2 Colas con prioridad

Los **algoritmos de las colas** con prioridad son muy conocidos en muchas áreas de la computación, por ejemplo, en los sistemas operativos multitareas, en los que ciertas aplicaciones deben tener prioridad sobre otras. Estos algoritmos también se utilizan en las colas con prioridad, cuando algunas clases de tráfico deben tener prioridad sobre otras.

El mecanismo de colas con prioridad se basa en la división de todo el tráfico de red en una pequeña cantidad de clases y en la asignación de alguna característica numérica a cada una de ellas, lo que se conoce como **prioridad**.

La **clasificación del tráfico** es una tarea independiente. Es posible atribuir a los paquetes clases de prioridad con base en diferentes características: dirección de destino, dirección de origen, identificador de la aplicación que ha generado este tráfico o cualquier combinación de las demás características contenidas en los encabezados de los paquetes. Las reglas de la clasificación de paquetes son parte de la **política de la administración de la red.**

Los **puntos de clasificación del tráfico** pueden residir en cada dispositivo de comunicaciones. Una solución más escalable consiste en delegar las funciones de clasificación de tráfico a uno o más dispositivos dedicados que se localicen en un extremo de la red. Por ejemplo, esta función puede delegarse a los switches de red corporativos, a los que las estaciones de trabajo del usuario final están conectadas o a los ruteadores de extremo de la red del proveedor del servicio. En este caso, es necesario incluir un campo especial en el paquete, el cual almacena el valor de prioridad asignado, de tal forma que los demás dispositivos de la red que procesan el tráfico después del dispositivo clasificador puedan utilizar esta información. Los encabezados de paquetes de la mayoría de los protocolos proporcionan dichos campos. Cuando el encabezado del paquete no tiene un campo especial de prioridad, se debe diseñar un protocolo adicional que incluya un nuevo encabezado que proporcione dicho campo. Dicha solución se seleccionó del protocolo Ethernet.

No solamente los switches y los ruteadores pueden asignar prioridades, sino también las aplicaciones que se ejecutan en el nodo de origen. También es necesario tener en cuenta que si no existe una política centralizada para asignar prioridades en la red, cada dispositivo de red podría no estar de acuerdo con la prioridad asignada al paquete por otro nodo de la red. En este caso, el dispositivo sobrescribirá el valor de la prioridad de acuerdo con la política local almacenada en dicho dispositivo.

Independientemente del método seleccionado de clasificación del tráfico, existen *varias* colas en el dispositivo de la red que soportan colas con prioridad. El número de dichas colas corresponde a la cantidad de clases de prioridad.[2] El paquete que arribó durante el periodo de congestión se coloca en la cola correspondiente a su clase de prioridad. La figura 7.9 muestra un ejemplo que ilustra el uso de cuatro colas de prioridad caracterizadas por alta, media, normal y baja prioridad. El dispositivo no procesará la cola con baja prioridad mientras la cola con la prioridad más alta contenga paquetes. Por lo tanto, los paquetes con prioridad media se procesan siempre y cuando la cola de paquetes con prioridad más alta se encuentre vacía. De acuerdo con esto, los paquetes con baja prioridad se procesan solamente cuando todas las colas de prioridades más altas (alta, media y normal) estén vacías.

En general, de manera predeterminada, a todas las colas de prioridad se les asignan memorias del mismo tamaño. Sin embargo, muchos dispositivos permiten que los administradores configuren de manera individual el tamaño de la memoria de cada cola. Éste determina el número máximo de paquetes que pueden almacenarse en una cola que tiene una prioridad específica. Si el paquete llega cuando la memoria está llena, éste se eliminará.

Como regla general, el *tamaño de la memoria* tiene un valor seguro cuando se manejan colas de longitud promedio; no obstante, es muy difícil evaluar este valor, ya que depende de la carga de la red. Debido a lo anterior, para lograr este objetivo es necesario supervisar de forma continua la operación de la red por periodos prolongados. En general, a medida

[2] A veces varias colas se representan mediante una cola que contiene solicitudes de diferentes clases. Si las solicitudes se recuperan de las colas de acuerdo con sus prioridades, sólo será otra representación del mismo mecanismo.

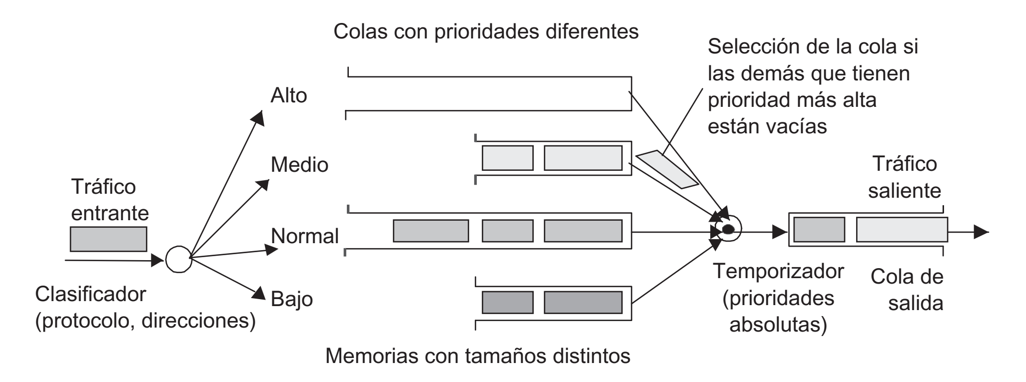


FIGURA 7.9 Colas con prioridad.

que es mayor la importancia del tráfico para el usuario, su velocidad y número de ráfagas también será mayor y en consecuencia será necesario un tamaño de memoria más grande. En el ejemplo que se presentó en la figura 7.9 se asignaron dispositivos con grandes cantidades de memoria para el tráfico con prioridades alta y normal; para las otras dos clases se asignaron dispositivos de memoria más pequeños. Para el tráfico de alta prioridad, lo que motivó esta solución es obvio. En cuanto al tráfico con prioridad normal, se espera que sea intenso y en ráfagas.

Las colas con prioridad garantizan un QoS alto para los paquetes de la cola que tenga la prioridad más alta. Si la velocidad promedio a la que estos paquetes llegan al dispositivo no excede el ancho de banda de la interfaz de salida (y el desempeño del procesador del dispositivo), los paquetes con la prioridad más alta siempre tendrán a su disposición el ancho de banda que requieren. El nivel de retardo de dichos paquetes es mínimo también, pero no es igual a 0 y depende principalmente de las características del flujo de dichos paquetes. A medida que las ráfagas del flujo y la velocidad de la información son mayores, será más grande la probabilidad de generación de la cola formada por paquetes de este tráfico de alta prioridad. El tráfico de las demás clases de prioridad es casi transparente para los paquetes con alta prioridad. Observe que al decir *casi*, esto implica que se pueden presentar situaciones en las cuales el paquete con más alta prioridad deba esperar hasta que el dispositivo termine el procesamiento del paquete con prioridad más baja. Esto sucede cuando la llegada del paquete con prioridad más alta coincide con el momento en el que el dispositivo comenzó a procesar el paquete con prioridad más baja.

En relación con otras clases de prioridad, el QoS que se les proporciona será menor que para los paquetes con la prioridad más alta. Observe que el grado con que se reduce esta calidad es difícil de predecir. Dicha reducción podrá ser muy significativa si el tráfico con la prioridad más alta es intenso. Si el coeficiente de utilización del dispositivo, determinado solamente por el tráfico de la más alta prioridad, se eleva a un valor cercano a 1 en instantes específicos, el tráfico de las clases con prioridad más baja prácticamente se congela en dichos intervalos.

Debido a esto, la cola con prioridad se utiliza cuando existe una clase de tráfico en tiempo real en la red, pero su intensidad no es elevada; en consecuencia, brindar servicio a esta clase no afecta proporcionárselo al resto del tráfico. Por ejemplo, el tráfico de voz es muy sensible a los retardos, aunque su velocidad rara vez excede de 8 a 64 Kbps. Por lo tanto, si se le asigna a este tráfico la prioridad más alta, el servicio ofrecido a las demás clases de tráfico no será degradado en forma significativa. No obstante, se pueden presentar otras situaciones; por ejemplo, considere una red en la que es necesario transmitir tráfico de video, el cual también

requiere servicio de prioridades, empero, tiene una velocidad significativamente más alta. En estos casos, se desarrollan algoritmos especiales de colas, los cuales ofrecen algunas garantías de que el tráfico de baja prioridad también será atendido, aun cuando la velocidad de las clases con prioridades más altas se incremente de manera significativa. Dichos algoritmos se estudian en la siguiente sección.

Los lectores observadores habrán notado que cuando se describen las colas con prioridad, se trabaja con clases de tráfico en vez de hacerlo con flujos individuales. Esta característica especial es muy importante y está relacionada no solamente con los algoritmos de colas con prioridad, sino también con otros mecanismos para garantizar el QoS.

La red puede atender tráfico con diferentes niveles de **granularidad**. Un flujo individual representa la unidad mínima de servicio que es tomada en cuenta por los mecanismos de QoS.

Si se garantizan los parámetros individuales del QoS de cada flujo, entonces se está trabajando con QoS a nivel de flujo. Si se combinan varios flujos dentro de un flujo común agregado y se deja de hacer una diferencia entre los flujos individuales cuando se garanticen los parámetros QoS, entonces se estará tratando con QoS a nivel clase de tráfico. Dichas clases también se llaman **agregados de tráfico.**

IMPORTANTE *Para combinar varios flujos en uno agregado, es necesario asegurar que éstos impongan los mismos requerimientos de QoS y tengan puntos de entrada y salida comunes hacia y desde la red.*

7.5.3 Colas ponderadas

El **algoritmo de colas ponderadas** se diseñó para brindar cierta cantidad mínima de ancho de banda a las clases de tráfico, o al menos para garantizar la observancia de algunos requerimientos de los retardos. La ponderación de una clase consiste en el porcentaje del ancho de banda total del recurso (por ejemplo, el procesador o interfaz de salida de un switch) que se garantiza para esta clase de tráfico.

De la misma forma que las colas con prioridad, las colas ponderadas requieren la división de tráfico en varias clases. Para cada una de ellas se genera una cola de paquetes por separado. Sin embargo, a las colas ponderadas, se les asigna el porcentaje del ancho de banda del recurso garantizado para esta clase en condiciones de saturación de recursos, más que una prioridad en específico. Para el flujo de entrada, el papel del recurso lo desempeña el procesador, y para el flujo de salida (una vez que se ha llevado a cabo la conmutación), es la interfaz de salida la que realiza este papel.

EJEMPLO *La figura 7.10 muestra un ejemplo en el que el dispositivo de red soporta cinco colas hacia la interfaz de salida. En condiciones de congestión, a dichas colas se les asigna 10%, 10%, 30%, 20% y 30% del ancho de banda de la interfaz de salida, respectivamente.*

Para lograr la meta formulada se brinda servicio a las colas de manera secuencial. En cada ciclo de servicio, se toma un número específico de bytes de cada cola, que corresponde a la ponderación de la misma. Si el ciclo de atención de la cola en el ejemplo considerado es igual a 1 segundo y la velocidad de la interfaz de salida es de 100 Mbps, en condiciones de congestión la primera cola obtendrá 10% del tiempo (es decir, 100 milisegundos) y, por lo tanto, 10 Mbits de datos se recuperarán de esa cola. El volumen de datos recuperados de la segunda cola será también de 10 Mbits. De acuerdo con esto, se recuperarán 30 Mbits de datos de la tercera cola, 20 Mbits de la cuarta y 30 Mbits de la quinta.

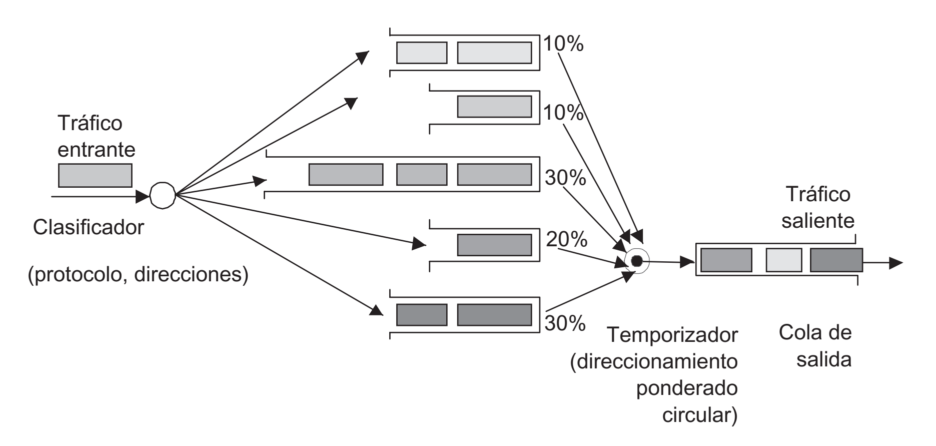


FIGURA 7.10 Colas ponderadas.

Como resultado, cada clase de tráfico obtendrá su ancho de banda mínimo garantizado. En la mayoría de las situaciones, es más deseable este resultado que al que las clases de tráfico de baja prioridad sean eliminadas por las de alta prioridad.

Como los datos son recuperados de la cola en forma de paquetes en lugar de bits, la distribución real del ancho de banda entre las clases de tráfico es siempre diferente de la planeada. Por ejemplo, la primera clase de tráfico puede recibir 9 o 12% en lugar de 10% en condiciones de congestión en la red.

A medida que el tiempo del ciclo es más prolongado, las proporciones requeridas entre las clases de tráfico se observan con más precisión. Esto sucede debido a que se selecciona un gran número de paquetes de cada cola y, por lo tanto, la influencia del tamaño de cada paquete es promediada.

Así, un ciclo prolongado da como consecuencia retardos significativos en la transmisión de paquetes. Por ejemplo, si el ciclo es igual a un segundo seleccionado del ejemplo que se presentó con anterioridad, el retardo podrá ser mayor que un segundo, pues el árbitro regresa a cada cola no más de una vez por segundo; además, cada cola contiene más de un paquete. Por lo tanto, cuando se selecciona la duración del ciclo, es necesario asegurar el balance entre la precisión de las proporciones del ancho de banda y el deseo natural de reducir el retardo.

En el ejemplo ofrecido, la duración del ciclo de trabajo de 1 000 μseg garantiza dicho balance; por otro lado, garantiza que la cola de cada clase sea atendida una vez cada 1 000 μseg. Asimismo, este tiempo es suficiente para recuperar varios paquetes de cada cola. En nuestro ejemplo, la primera cola tendrá 100 μs, tiempo suficiente para transmitir una trama de Fast Ethernet o 10 tramas de Gigabit Ethernet a la red.

Cuando se emplea el algoritmo de colas ponderadas, el coeficiente de utilización para el tráfico de una clase específica influye de manera significativa en el retardo y en los valores de variación del retardo del paquete de esta clase. En este caso, el coeficiente se calcula como el cociente entre la velocidad de entrada de una clase específica de tráfico y el ancho de banda asignado a esa clase de acuerdo con su peso. Por ejemplo, si asignamos 10% del ancho de banda total de la interfaz de salida a la primera cola (es decir, 10 Mbps) y la velocidad promedio del flujo que cae en esta cola es de 3 Mbps, el coeficiente de utilización para este flujo será de 3/10 = 0.3. La dependencia que se muestra en la figura 7.5 indica que los retardos serán insignificantes con respecto al valor del coeficiente de utilización. Si la velocidad del flujo de entrada de esta cola fuera de 9 Mbps, la cola crecería de forma importante. Si se

excede el límite de 10 Mbps, parte del flujo de paquetes se eliminará constantemente debido a la saturación de la cola.

El comportamiento cualitativo de la cola y, en consecuencia, de los retardos parece muy similar al de la cola FIFO —esto es, a medida que el coeficiente de utilización es menor, la longitud promedio de la cola y los retardos también lo son—.

De la misma manera que las colas con prioridad, cuando se emplean colas ponderadas, el administrador puede asignar de forma manual diferentes tamaños de memoria para las distintas clases de colas. La reducción en el tamaño de la memoria para las colas aumentará el número de paquetes perdidos en condiciones de congestión; sin embargo, se reducirán los tiempos de espera de los paquetes que no fueron eliminados.

Existe otro tipo de colas ponderadas: **colas ponderadas justamente** *(WFQ). En este caso, el ancho de banda del recurso se divide entre todos los flujos de manera equitativa (es decir, justa).*

NOTA *Las colas ponderadas aseguran las relaciones requeridas entre las velocidades de tráfico de diferentes colas sólo durante periodos de congestión, cuando cada cola se llena a un ritmo constante. Si cualquiera de las colas está vacía (lo cual significa que, para el tráfico de esta clase, el periodo actual no es el de congestión), esta cola se suprimirá durante la inspección secuencial actual y el tiempo asignado para atender esta cola se distribuirá entre las demás de acuerdo con el peso de cada una. Por lo tanto, durante periodos específicos, el tráfico de una clase determinada puede tener una velocidad mayor que el porcentaje apropiado del ancho de banda de la interfaz de salida.*

7.5.4 Algoritmos híbridos de las colas

Cada uno de los métodos que se describieron tiene sus ventajas y desventajas. Las colas con prioridad garantizan mínimos niveles de retardo, al menos para el tráfico de más alta prioridad. Este algoritmo atiende el tráfico de las colas de prioridad más elevada, sin importar si su velocidad es muy grande y no proporciona ninguna garantía en relación con el ancho de banda promedio del tráfico proveniente de las colas de prioridad más baja.

Las colas ponderadas garantizan la velocidad promedio del tráfico, pero no proporcionan ninguna garantía respecto a los retardos.

Existen también algoritmos híbridos de colas que tratan de llegar a un compromiso entre dichos métodos. El más popular de ellos utiliza una cola con prioridad y atiende a las demás de acuerdo con el algoritmo ponderado. En general, las colas con prioridad se usan con tráfico en tiempo real y otras más se emplean con tráfico elástico de diversas clases. A cada clase de tráfico elástico se le asigna una cantidad mínima garantizada de ancho de banda durante los periodos de congestión. Dicha cantidad mínima se calcula como un porcentaje del ancho de banda que quede después de atender el tráfico con prioridad. Obviamente, es necesario limitar el tráfico prioritario de alguna forma con el fin de evitar que éste consuma todo el ancho de banda del recurso. Como regla general, esto se logra mediante el uso de **herramientas para perfilar el tráfico**, las cuales se estudiarán más adelante en este capítulo.

7.6 RETROALIMENTACIÓN

PALABRAS CLAVE: mecanismo para el control de la congestión, congestión de la red, mecanismo de retroalimentación, reservación, indicación de congestión, velocidad máxima de transmisión, crédito e información implícita.

7.6.1 Propósito

Los algoritmos de administración de colas son herramientas obligatorias para evitar la congestión de la red; sin embargo, dichas herramientas no son suficientes. Los algoritmos interpretan la situación *como es* y hacen su mejor esfuerzo para mejorar la situación y lograr una distribución justa de recursos en condiciones de escasez de ellos. No obstante, dichos algoritmos no pueden eliminar la escasez de ancho de banda. Estos mecanismos se clasifican como **mecanismos para el control de la congestión** y se activan cuando la red funciona en condiciones de congestión.

Existe otra clase de herramientas que intentan predecir y **evitar la congestión de la red,** y se denominan *mecanismos para evitar la congestión*. El principal objetivo de dichas herramientas consiste en prevenir situaciones de congestión, debido a que es mucho mejor transmitir datos a una velocidad baja pero sin pérdidas que a velocidades altas y perder paquetes durante periodos de congestión.

La prevención de la congestión de la red es posible sólo cuando la velocidad total de los flujos de datos transmitidos utilizando cada interfaz de los switches de la red es menor que el ancho de banda de esa interfaz. Se pueden poner en práctica dos métodos con el fin de alcanzar este objetivo: aumentar el ancho de banda de la interfaz o reducir las velocidades de los flujos. El primer método está relacionado con el diseño de la red y las herramientas de planeación y no se estudiará aquí.

El segundo método puede ponerse en marcha mediante el uso de dos procedimientos diferentes. Uno de ellos se basa en la explotación del **mecanismo de retroalimentación** que el nodo de red congestionado utiliza para solicitar a los nodos anteriores ubicados a lo largo de la ruta de tráfico (o los flujos pertenecientes a la misma clase de tráfico) que reduzcan temporalmente su velocidad de tráfico. Cuando ya no existe congestión en dicho nodo, éste envía otro mensaje y permite aumentar la velocidad de transmisión de datos. Tal método no requiere un conocimiento previo de la intensidad de tráfico, sino simplemente reacciona ante la congestión y asume que los protocolos que operan en todos los nodos reaccionarán al mensaje informándoles de la congestión y reducirán la velocidad de tráfico.

Otro método se basa en la **reservación** del ancho de banda para los flujos que circulan a través de la red. Este método requerirá información preliminar acerca de las velocidades de los flujos, así como actualizaciones de dicha información si sus magnitudes cambian. Los principios de la reservación de recursos se estudiarán con más detalle en la siguiente sección. Por el momento, concentrémonos en los mecanismos de retroalimentación.

7.6.2 Participantes de la retroalimentación

Existen varios tipos de mecanismos de retroalimentación, los cuales difieren en la información proporcionada por la retroalimentación, así como en el tipo de nodo que genera dicha información y la clase de nodo que reacciona a éste, ya sea que se trate de un nodo terminal (computadora) o de un nodo de tránsito (switch o ruteador).

La figura 7.11 muestra varios métodos que pueden utilizarse para organizar la retroalimentación.

La *retroalimentación 1* está organizada entre dos nodos terminales de red y representa el método más radical para reducir las cargas en la red, ya que sólo los nodos terminales (emisores) pueden reducir la velocidad a la que se envía la información a la red. Sin embargo, este tipo de retroalimentación no está clasificada como un método de control de la congestión, ya que su objetivo principal es reducir las cargas en el nodo de destino más que en los dispositivos de red. En principio, éste es el mismo problema, pues surge debido a que la velocidad

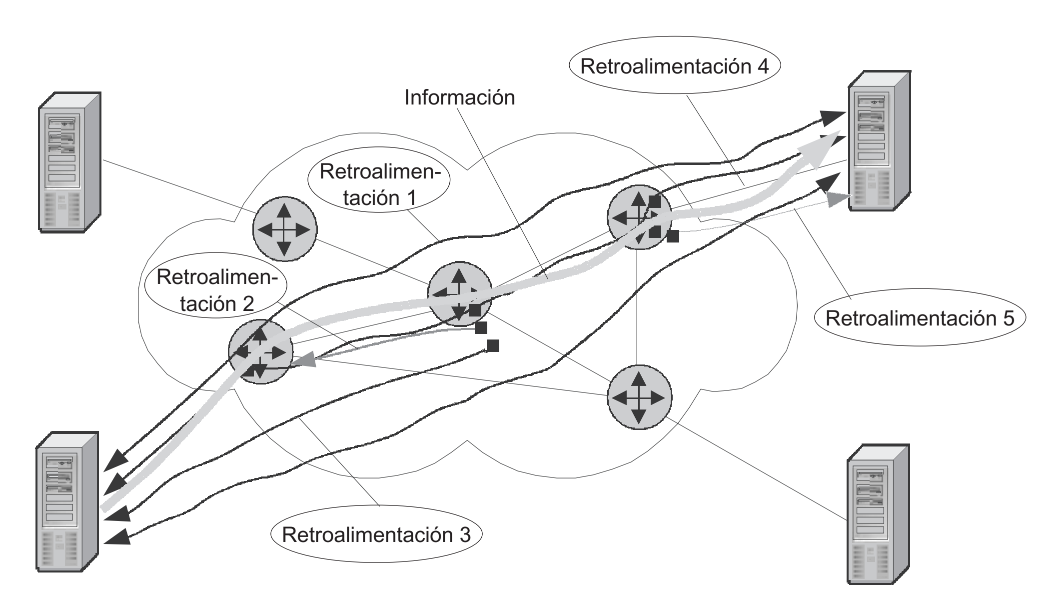


FIGURA 7.11 Participantes de la retroalimentación.

a la cual llegan los paquetes al recurso de la red excede de manera temporal a la velocidad a la que este recurso las procesa. Sin embargo, en este caso, el switch no desempeña el papel de recurso de la red, sino que es el nodo terminal. Tradicionalmente, este tipo de retroalimentación se llama *flujo de control*. Los dispositivos de la red no participan en la operación de este tipo de mecanismo de retroalimentación y solamente envían los mensajes apropiados entre los nodos terminales. A pesar de tener nombres diferentes, los métodos para el control de la congestión y aquellos para el control de flujo utilizan mecanismos similares.

Cuando se organiza la retroalimentación, es necesario tener en cuenta el tiempo requerido para transmitir información a través de la red. En las WAN de alta velocidad, el nodo de origen puede transmitir miles de paquetes durante el tiempo requerido para transferir el mensaje e informarle que el nodo de destino está saturado. Por lo tanto, la saturación no se eliminará a tiempo.

A partir de la teoría del control automático, se sabe que los retardos en el circuito de retroalimentación pueden producir muchos efectos indeseables contrarios a las intenciones iniciales. Por ejemplo, se podrán iniciar procesos oscilatorios en el sistema si se evita que éste vuelva al estado de equilibrio. En las etapas iniciales de la evolución de Internet, dicho fenómeno no era raro. Por ejemplo, debido a la imperfección de los algoritmos de retroalimentación y de enrutamiento, aparecieron zonas de saturación y se movían periódicamente a través de la red. La razón de dicho problema es evidente: los retardos en el circuito de retroalimentación proporcionaban al elemento controlador información obsoleta acerca del estado del elemento controlado.

En este caso, el nodo de origen obtiene información acerca del estado de la cola del nodo de destino que presenta el retardo. Por lo tanto, es posible una situación en la que el nodo de origen empiece a reducir la velocidad de transmisión, aunque esto no sea necesario debido a que no hay ninguna cola en el nodo de destino. A veces, el nodo de origen, una vez que ha recibido la información acerca de los retardos, empieza a aumentar la velocidad de información cuando el nodo de destino comienza a experimentar una sobrecarga. Para eliminar dichos efectos, generalmente se incluye un elemento integrador en el circuito de retroalimentación.

Esta unidad integradora tiene en cuenta no sólo el mensaje de retroalimentación actual, sino también algunos mensajes anteriores con el fin de conocer la dinámica de los cambios de esta situación y reaccionar apropiadamente.

La *retroalimentación 2* se organiza entre dos switches vecinos. El switch informa a su vecino (considerando un flujo determinado) que pasa por una congestión y su memoria está saturada al valor crítico. Una vez que haya recibido dicho mensaje, el vecino deberá reducir temporalmente la velocidad de transmisión de datos en la dirección del switch congestionado, eliminando así el problema de la congestión. Esta solución es menos eficaz para toda la red, ya que el flujo podría continuar abandonando el nodo de origen a la misma velocidad que antes. Para el switch que experimenta congestión, ésta aún es una buena solución, pues tendrá tiempo para descargar la cola saturada. Sin embargo, el problema se transferiría al switch vecino, donde podría aparecer la sobrecarga, ya que comenzaría a transmitir datos de su memoria a una velocidad menor. La ventaja de este método es su bajo retardo de retroalimentación, dado que ambos nodos son vecinos, siempre y cuando no estén conectados a través de un canal satelital.

La *retroalimentación 3* está organizada entre el switch de tránsito y el nodo de origen. A pesar de que los mensajes de retroalimentación son transmitidos por varios switches de tránsito en la dirección del nodo de origen, dichos switches no reaccionan a éste.

La *retroalimentación 4* representa el caso más general (figura 7.11). Aquí, el mensaje acerca de la sobrecarga es generado por el nodo de destino y enviado al nodo de origen, de forma similar al primer caso. No obstante, este caso es diferente en el sentido de que cada switch de tránsito reacciona a este mensaje. Primero, este método reduce la velocidad de transmisión de datos en la dirección del nodo de destino y, segundo, permite el cambio del contenido del mensaje a través del circuito de retroalimentación. Por ejemplo, si el nodo de destino solicita reducir la velocidad a 30 Mbps, el switch de tránsito podrá reducir este valor a 20 Mbps después de evaluar el estado de su memoria. La versatilidad de este método reside en que no solamente el nodo de destino, sino también cualquiera de los switches de tránsito pueden generar el mensaje de retroalimentación.

Al describir las distintas versiones en las que se organiza la retroalimentación, se ha supuesto que el mensaje de sobrecarga viaja en la dirección opuesta al sentido de la transmisión de información del usuario; empero, algunos protocolos de comunicaciones no ofrecen la posibilidad de que los nodos de tránsito generen dichos mensajes. En estas condiciones se utiliza una técnica artificial —esto es, la transmisión del mensaje acerca de la congestión al nodo de destino, el cual lo transforma en un mensaje de retroalimentación y lo envía en la dirección que se requiera (es decir, hacia el nodo de origen)—. Esta variante se muestra en la figura 7.11 como *retroalimentación 5*.

7.6.3 Información de la retroalimentación

Los métodos de retroalimentación empleados en la actualidad utilizan los siguientes tipos de información:

- Indicación de congestión.
- Velocidad máxima de transmisión.
- Máxima cantidad de datos (crédito).
- Información implícita.

Indicación de congestión: no contiene el nivel de congestión de nodo o de red, sino simplemente reporta la congestión. Las reacciones del nodo que recibe dicho mensaje

pueden ser diferentes. En algunos protocolos, el nodo deja de transmitir información en un sentido específico hasta que recibe otro mensaje de retroalimentación, permitiéndole continuar la transmisión. En otros protocolos, el nodo se comporta de manera adaptable: reduce la velocidad a un valor específico y espera la respuesta de la red. Si los mensajes de retroalimentación que contienen las indicaciones de congestión continúan llegando, el nodo seguirá reduciendo la velocidad de transmisión.

Máxima velocidad de transmisión. El segundo tipo de mensajes utiliza indicaciones acerca del umbral de velocidad que el nodo de origen o de tránsito debe observar. Éste es un método más preciso que el anterior para el control de la congestión, ya que informa explícitamente a su vecino acerca de a qué nivel deberán disminuir la velocidad de transmisión. Es obligatorio que la red tenga en cuenta el tiempo de transmisión del mensaje con el fin de eliminar oscilaciones en la red, asegurando así la respuesta requerida a la congestión. Por lo tanto, en las WAN, este método generalmente está implementado como el de retroalimentación 4 que se proporcionó en el ejemplo anterior, y hace uso de todos los switches de la red.

Máximo volumen de datos. El último tipo de mensajes está relacionado con el algoritmo de ventana deslizante que se utiliza ampliamente en las redes de conmutación de paquetes. El algoritmo de ventana deslizante se estudió con anterioridad en este capítulo y no sólo permite que se garantice la transmisión confiable de datos, sino también da la posibilidad de organizar la retroalimentación para el control de flujo (si es que ésta se encuentra organizada entre nodos terminales) o para el control de la congestión (si la retroalimentación se organiza entre switches de red).

El parámetro que transporta la información de retroalimentación es la ventana deslizante actual (cuando se describieron los principios de operación de este mecanismo, se le designó como W). La mayoría de los protocolos que ponen en práctica el algoritmo de ventana deslizante cuentan con la infraestructura para indicar el tamaño de ventana actual de los reconocimientos y confirman la recepción de la siguiente porción de los datos. Esta información acerca del tamaño actual de la ventana corresponde al estado actual del modo de recepción.

Dicho parámetro también se llama *crédito* y es proporcionado al nodo emisor por el nodo receptor. El nodo emisor puede enviar un volumen específico de información (o cierto número de paquetes, si el tamaño de la ventana se mide así) correspondiente al crédito. Si se termina dicho crédito, el nodo emisor no tiene derecho a transmitir información alguna hasta que reciba el siguiente crédito. En estas condiciones de congestión, el nodo receptor reduce el tamaño de ventana y disminuye así la carga. Si se elimina la congestión, el nodo receptor aumentará el tamaño de la ventana otra vez.

La aplicabilidad de ese algoritmo es limitada, debido a que opera solamente cuando se utilizan los protocolos orientados a la conexión.

Información implícita. Este método se basa en el principio según el cual el nodo emisor decide que el nodo o nodos receptores están saturados, con base en algunas indicaciones implícitas sin utilizar los mensajes directos de retroalimentación. Por ejemplo, la pérdida de paquetes puede servir como indicación implícita. Para detectar la pérdida de paquetes, el protocolo debe estar orientado a la conexión; siempre que así sea, el tiempo de expiración o la llegada del reconocimiento positivo duplicado podrán interpretarse como una evidencia implícita de la pérdida de paquetes. Sin embargo, dicha pérdida no siempre es evidencia de la congestión de la red. De hecho, la congestión de la red es solamente una de las posibles razones de la pérdida de paquetes. La lista de los demás motivos por los que esto puede darse incluye causas como la operación poco confiable de los dispositivos de comunicación,

entre las que se cuentan la falla de hardware y la distorsión de los datos debida al ruido. No obstante, como la reacción a la congestión y a la operación poco confiable de la red debe ser la misma —es decir, una reducción en la velocidad de transmisión—, la ambigüedad de las causas de las pérdidas de paquetes no representa ningún problema.

Un ejemplo de un protocolo que utiliza información implícita acerca de la congestión es el protocolo TCP. Éste utiliza información explícita de retroalimentación (el tamaño de la ventana) cuando controla el flujo e información implícita (pérdidas de paquetes y reconocimientos duplicados) cuando controla la congestión. En el primer caso, el nodo de origen fija el tamaño de la ventana al valor especificado por el nodo de destino. En el segundo caso, el nodo de origen decide por sí mismo en qué nivel es necesario reducir la ventana para disminuir el efecto de la congestión de la red o como reacción a la baja confiabilidad de la transmisión.

7.7 RESERVACIÓN DE RECURSOS

PALABRAS CLAVE: QoS, formateo del tráfico, política del tráfico, clasificación del tráfico, mecanismos de acondicionamiento del tráfico, protocolo de reservación de recursos (RSVP), circuito virtual, perfil de tráfico, y mecanismos para atender las colas.

7.7.1 Reservación de recursos y conmutación de paquetes

La reservación de recursos representa una alternativa del mecanismo de retroalimentación, el cual también se clasifica como una herramienta para evitar la congestión. Pero en vez de intentar reaccionar a la congestión sin alguna estrategia, el mecanismo de reservación de recursos intenta limitar el nivel de congestión a un valor aceptable. Dicho valor debe garantizar que los algoritmos para controlar la congestión que están implementados en los switches de la red sean capaces de manejar las sobrecargas a corto plazo y de brindar los valores de los parámetros QoS requeridos sin utilizar el mecanismo de retroalimentación.

La reservación de recursos en las redes de conmutación de paquetes es básicamente distinta de un procedimiento similar en las redes de conmutación de circuitos. En estas últimas, una parte fija del ancho de banda del canal físico está reservada para cada conexión (circuito). El flujo se transmite a través de la red a una velocidad constante igual al ancho de banda reservado y esta velocidad es equivalente a la máxima velocidad del flujo. El ancho de banda del circuito está siempre reservado para este flujo y no puede redistribuirse de manera dinámica a otro flujo. Sin la reservación previa de recursos, las redes de conmutación de circuitos simplemente no pueden operar, lo cual constituye su principio básico.

En las redes de conmutación de paquetes, la reservación de recursos no es obligatoria; sin embargo, cuando ésta se realiza, el procedimiento es diferente respecto a la reservación de recursos en las redes de conmutación de circuitos, al menos dos aspectos:

- La reservación se lleva a cabo en la velocidad promedio del flujo.
- El ancho de banda puede redistribuirse de manera dinámica entre dos flujos diferentes.

La reservación consiste en solicitar todos los recursos a lo largo de la ruta del flujo, con el fin de verificar que la velocidad sostenida del flujo no exceda el desempeño de los mismos. Si se satisface esta condición, cada recurso recuerda que tendrá que dejar pasar este flujo y que se le asignaron partes específicas de su desempeño.

EJEMPLO: *Considere el ejemplo del procedimiento de reservación de recursos (figura 7.12). Suponga que en el estado inicial, los recursos de la red no estaban reservados. Posteriormente, decidimos asignar algunos recursos de la red al flujo 1; para lograrlo, debemos saber al menos la velocidad promedio del flujo requerida. Suponga que la velocidad sostenida del flujo es de 15 Mbps y que los valores del ancho de banda de todos los enlaces de comunicaciones (y, en consecuencia, de las interfaces de los switches) son de 100 Mbps. Para efectos de simplicidad, considere que cada interfaz de entrada está equipada con un procesador integrado y que su desempeño excede el ancho de banda de su interfaz.*

Siempre y cuando se cumplan estos requerimientos, el procesador no se convertirá en un cuello de botella. Por lo tanto, hay que tener en cuenta el ancho de banda de las interfaces de salida sólo cuando se tome una decisión relacionada con la reservación de recursos.

El flujo 1 puede usarse para dar servicio, ya que todas las interfaces a lo largo de su ruta tienen un ancho de banda suficiente para atender este flujo (15 < 100). Por ende, se lleva a cabo la reservación y cada interfaz a lo largo de la ruta del flujo recuerda que ha asignado 15 Mbps de su ancho de banda al flujo 1.

Ahora suponga que cierto tiempo después es necesario hacer una reservación para el flujo 2, el cual está caracterizado por tener una velocidad sostenida de 70 Mbps. Dicha reservación también puede hacerse, ya que todas las interfaces a lo largo de la ruta del flujo 2 tienen un ancho de banda disponible (no reservado para otro flujo) de más de 70 Mbps. Las interfaces a través de las cuales pasan tanto el flujo 1 como el 2 (interfaces i3/S2 e i1/S3) tenían 85 Mbps de ancho de banda disponible y las demás interfaces 100 Mbps. Después de la reservación, las interfaces i3/S2 e i1/S3 tendrán 15 Mbps de ancho disponible cada una.

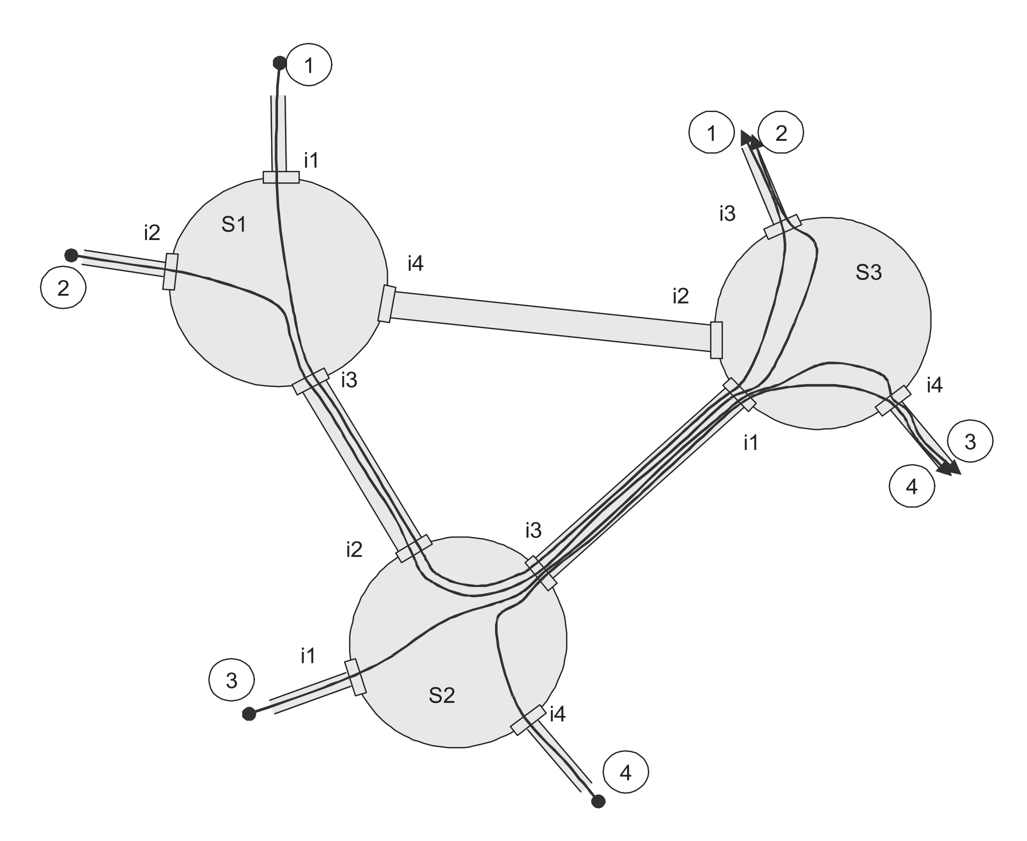


FIGURA 7.12 Reservación de recursos en las redes de conmutación de paquetes.

El intento de reservar un ancho de banda para el flujo 3 demostró tener éxito. La velocidad sostenida de este flujo es de 10 Mbps; sin embargo, un intento de reservación de recursos para el flujo 4, el cual tiene una velocidad sostenida de 20 Mbps, fallará, ya que las interfaces i3/S32 e i1/S3 solamente contarán cada una con 5 Mbps de ancho de banda disponible.

El ejemplo muestra que la red se rehusará a atender el flujo si no puede garantizarle el nivel de QoS requerido. Desde luego, se ha simplificado el esquema de reservación de recursos, ya que lo que es de interés es la idea principal de este mecanismo. En la práctica, no solamente la red es capaz de garantizar la velocidad de flujo promedio, sino también otras características del QoS, como el retardo máximo, la variación máxima del retardo y el nivel permitido de pérdida de datos. No obstante, para lograr lo anterior, la red debe conocer algunos parámetros adicionales del flujo —por ejemplo, el nivel máximo de ráfagas—, con la finalidad de reservar al espacio de memoria requerido.

Al reservar recursos, se debe tener en cuenta determinado ancho de banda disponible para el tráfico sensible al retardo y para el tráfico elástico de manera separada. Para garantizar un nivel aceptable de retardos y sus variaciones para el tráfico sensible al retardo, el ancho de banda total máximo reservado no debe exceder 50% del ancho de banda total de cada recurso. Como el lector recordará, en este caso, en condiciones de colas con prioridad, dicho tráfico experimentará un pequeño nivel de retardo. Esta aseveración se ilustra mediante el ejemplo considerado. Suponga que se decidió reservar 30% del ancho de banda de los recursos para el tráfico sensible al retardo. Entonces, si los flujos 1 y 3 son sensibles a los retardos, la reservación será factible; por otro lado, si los flujos 1 y 2 son sensibles a los retardos, la reservación no será factible, ya que la velocidad promedio total de dichos flujos es de 85 Mbps, la cual es mayor al 30% de 100 Mbps (30 Mbps).

Si se supone que el tráfico sensible al retardo será atendido en la cola de prioridad, cuando se reserve el ancho de banda para el tráfico elástico será necesario considerar que solamente la parte del ancho de banda que quede después del tráfico sensible al retardo puede reservarse para éste. Por ejemplo, si los flujos 1 y 3 son sensibles a los retardos y se les ha asignado el ancho de banda requerido, solamente 70 Mbps del ancho de banda no reservado estará disponible a los flujos elásticos.

¿Qué pasa después de que ocurre la reservación de recursos en algunos flujos de la red? Básicamente no pasa nada a nivel del procesamiento de paquetes. La única diferencia entre las redes con y sin reservación de recursos es que la primera está cargada de manera racional. Lo que sí es cierto es que dicha red no contiene recursos que operen en modo de congestión.

Los mecanismos de colas continúan su trabajo y garantizan el almacenamiento temporal de paquetes durante los periodos de ráfagas. Debido a que se planearon cargas de recursos con base en velocidades promedio, las velocidades de flujo durante los periodos de ráfagas pueden, por algunos periodos muy cortos, exceder las velocidades promedio. Por lo tanto, los métodos para controlar la congestión aún son necesarios. Con el fin de garantizar las velocidades de flujo promedio que se requieren durante los periodos de congestión, será posible atender dichos flujos si se utilizan las colas ponderadas.

La ventaja principal del método de conmutación de paquetes se conserva. Si cierto flujo no utiliza totalmente el ancho de banda que se le asignó, tal ancho de banda podrá usarse para atender otro flujo. Es una práctica muy común reservar un ancho de banda solamente en forma parcial para todos los flujos. La parte restante de los flujos será atendida sin reservación, obteniendo el servicio basado en el mejor esfuerzo. De manera temporal, el ancho de banda disponible puede emplearse dinámicamente para atender dichos flujos, sin violar sus obligaciones de atender flujos sin reservación.

Las redes de conmutación de circuitos no pueden llevar a cabo dicha redistribución de recursos, ya que éstas no cuentan con unidades de información con direcciones independientes, como los paquetes.

EJEMPLO *Ahora se verá la diferencia principal entre la reservación de recursos en las redes de conmutación de paquetes y de circuitos con un ejemplo de tráfico de automóviles. Suponga que en alguna ciudad las autoridades locales deciden garantizar algunos privilegios para las ambulancias. Durante la discusión del proyecto, se sugieren dos ideas opuestas: la primera consiste en dedicar un carril independiente para las ambulancias en todos los caminos, en el cual los demás vehículos no tienen derecho a circular, aun cuando no haya ambulancias en dicho camino.*

El segundo método también sugiere dedicar un carril independiente para las ambulancias; sin embargo, los demás medios de transporte tienen derecho a usarlo siempre que no haya ambulancias en ese momento. Si aparece una ambulancia, todos los vehículos que circulen por el carril privilegiado tienen que dejarlo libre inmediatamente. Como se observa con claridad, la primera variante corresponde a la reservación de recursos en las redes de conmutación de circuitos, ya que en dichas redes el carril dedicado es utilizado exclusivamente por ambulancias, lo necesiten o no. El segundo método es análogo a la reservación de recursos en las redes de conmutación de paquetes. En este caso, la eficacia del camino se utiliza de manera más eficiente. Dicha variante es menos favorable para las ambulancias, pues los vehículos no privilegiados representan obstáculos para ellas.

Si se retoma la analogía de las redes de conmutación de paquetes, es necesario hacer énfasis en que, para asegurar las garantías de servicio en cada flujo, el esquema de reservación descrito no es suficiente.

Se ha supuesto que la velocidad promedio y los parámetros de las ráfagas de los flujos se conocen con exactitud. En la práctica, dicha información no siempre es confiable. ¿Qué pasará si el flujo es transferido a la red a una velocidad que exceda a la que se tuvo en cuenta cuando se llevó a cabo la reservación de recursos? Existe otra pregunta al respecto que se halla sin respuesta: ¿cómo puede garantizarse la reservación automática de ancho de banda a lo largo de la ruta del flujo?

Para resolver los problemas que se acaban de formular, es necesario contar con un sistema de herramientas de QoS que incluyan mecanismos aparte de los algoritmos de colas.

7.7.2 Sistema QoS basado en reservaciones

El sistema QoS tiene una naturaleza distribuida, ya que sus elementos deben estar presentes en todos los dispositivos de red que llevan a cabo el envío de paquetes: switches, ruteadores y servidores de acceso. Por otro lado, es necesario coordinar la operación de los dispositivos de red individuales cuyo objetivo consiste en garantizar el soporte QoS. Esto es necesario para asegurar que el QoS sea el mismo a lo largo de toda la ruta en la que viajan los paquetes. Por esta razón, el sistema QoS debe también incluir elementos de administración centralizada y permitir a los administradores de la red coordinar el proceso de configurar los mecanismos QoS en los dispositivos de red independientes.

El sistema QoS basado en la reservación de recursos abarca varios tipos de mecanismos (figura 7.13):

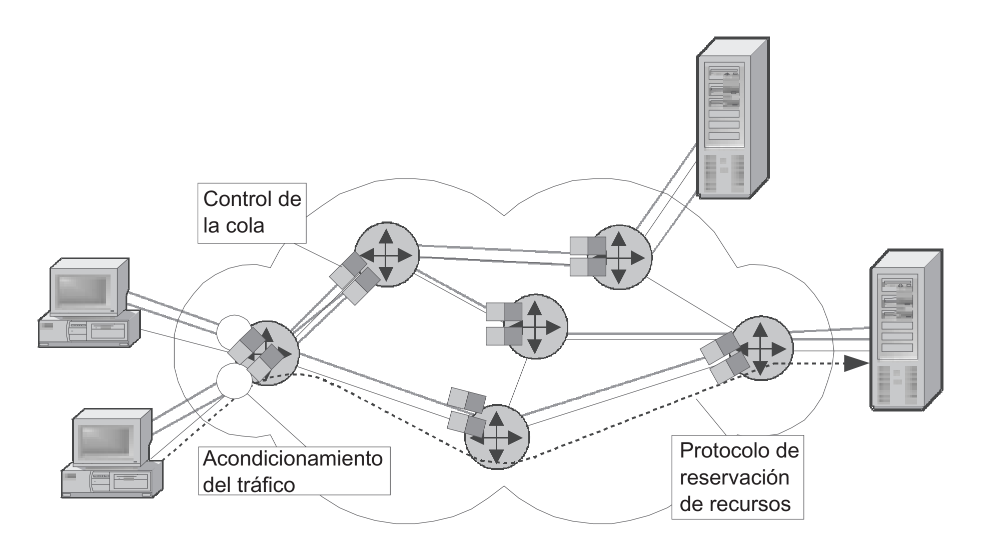


FIGURA 7.13 Arquitectura de un sistema QoS basado en la reservación.

- Mecanismos para la atención de las colas.
- Protocolo para la reservación de recursos.
- Mecanismos para el acondicionamiento del tráfico.

Los **mecanismos para la atención de las colas** se utilizan para la operación durante periodos de congestión temporal. Las colas ponderadas se usan para atender el tráfico elástico; para el tráfico en tiempo real, se emplean las colas con prioridad. Para reducir la carga en los switches y ruteadores, se usa el servicio por clases de tráfico, ya que es necesario soportar un número significativamente más pequeño de colas y almacenar menos información acerca del estado de los flujos.

El **protocolo de reservación** es necesario para automatizar el procedimiento de reservación de recursos a lo largo de la ruta de algún flujo (es decir, de extremo a extremo). Los protocolos de reservación son análogos a los que se requieren para establecer la conexión en las redes de conmutación de circuitos. Por lo tanto, a menudo se les llama *protocolos de señalización*, de acuerdo con los términos que se utilizan en este tipo de redes.

El protocolo de reservación de recursos efectúa dos recorridos a través de la red. Primero, pasa desde el emisor de la información hasta el receptor de ella. El mensaje del protocolo de reservación especifica el llamado **perfil de tráfico**, el cual incluye características como la velocidad promedio, los parámetros de las ráfagas y los requerimientos del nivel de retardo. Con base en este perfil, cada switch a lo largo de la ruta del flujo decide si puede o no llevar a cabo la reservación para este flujo. Si está de acuerdo en hacer la reservación, el mensaje se seguirá transmitiendo y el switch almacenará información acerca de éste. Si todos los switches a lo largo de la ruta están de acuerdo con la reservación solicitada, el último switch enviará un nuevo mensaje acerca del protocolo de reservación de recursos. Este nuevo mensaje viaja en sentido contrario. Como dichos mensajes pasan por los switches, cada uno de ellos registra el estado de reservación para este flujo.

Tanto el nodo terminal como un dispositivo de tránsito pueden iniciar la operación del protocolo de reservación de recursos. En este caso, el servicio garantizado del flujo tendrá lugar no sólo a lo largo de la ruta del tráfico, sino también dentro de los límites de la región específica de la red, lo cual seguramente reducirá el QoS proporcionado al tráfico.

El protocolo de reservación puede llevar a cabo una reservación para los flujos individuales y para las clases de tráfico. Los principios de su operación en cada caso permanecen iguales. Sin embargo, de acuerdo con la clase de tráfico, el papel de iniciador de la reservación no lo realiza el nodo terminal, el cual está interesado principalmente en su propio flujo, sino uno de los switches de la red. Como regla general, éste es uno de los switches de orilla de la red del proveedor del servicio, el cual recibe flujos provenientes de diversos usuarios.

En las redes con circuitos virtuales, las funciones del protocolo de reservación de recursos son generalmente llevadas a cabo por el protocolo **para establecer un circuito virtual.** Cabe mencionar que el protocolo de establecimiento de la conexión por sí mismo no puede realizar la reservación de recursos, ya que ésta es una función opcional de dicho protocolo. En las redes de datagramas, el protocolo de reservación es independiente. Un ejemplo de dicho protocolo es el **protocolo para la reservación de recursos** (**RSVP**), el cual trabaja con las redes IP.

Las reservaciones pueden llevarse a cabo aun sin el protocolo de reservación. Para hacer esto, los administradores de red deben configurar de forma manual los parámetros de cada flujo en todos los switches de la red.

Los **mecanismos de acondicionamiento de tráfico** supervisan los parámetros actuales del flujo y aseguran que correspondan a los valores declarados durante la reservación. Son como un tipo de puntos de prueba que verifican el tráfico antes de que éste ingrese al switch. Sin dichos mecanismos, sería imposible garantizar el QoS requerido para el tráfico, ya que si las velocidades promedio del flujo o las ráfagas exceden el nivel declarado en el momento de la reservación, los retardos y pérdidas de paquetes excederán también el nivel requerido del flujo. Esto puede pasar por varias razones. Primero, es difícil realizar evaluaciones precisas de los parámetros del tráfico. Las mediciones preliminares de las velocidades promedio y de las ráfagas pueden generar resultados imprecisos debido a que estas características pueden variar con el tiempo, por lo que una semana después los resultados que se midieron pueden no corresponder a la realidad. Además, las distorsiones de los parámetros del tráfico hechas con toda intención no deben pasarse por alto, en especial cuando se utilizan servicios comerciales.

El mecanismo para el acondicionamiento del tráfico generalmente incluye varias funciones:

- **Clasificación del tráfico**. Esta función selecciona paquetes del mismo flujo que tengan los mismos requerimientos de QoS de la secuencia de paquetes que llega al dispositivo. En las redes que contienen circuitos virtuales no se requiere una clasificación adicional, pues la etiqueta del circuito virtual indica el flujo específico. En las redes de datagramas, como regla general, no existen tales indicaciones; por lo tanto, la clasificación se lleva a cabo con base en diferentes características formales de los paquetes: direcciones de origen y destino, identificadores de aplicación, etc. Sin la clasificación de paquetes, es imposible asegurar el soporte QoS en las redes de datagramas.
- **Políticas de tráfico.** Por cada flujo de entrada, en cada switch existe un conjunto de parámetros QoS apropiado conocidos como perfiles de tráfico. La política asume la verificación de la correspondencia entre cada flujo de entrada con los parámetros de dicho perfil. Existen algoritmos que permiten llevar a cabo esta verificación en forma automática a la misma velocidad a la que llegan los paquetes a la interfaz de entrada del switch. Algunos ejemplos de algoritmos de política son el de *la cubeta de filtración* y el de *la cubeta de estafeta*. Dichos algoritmos se estudiarán con más detalle cuando se describan las tecnologías individuales, como IP, Frame Relay y ATM.

Si los parámetros del perfil se violan (por ejemplo, si el tamaño de ráfaga o la velocidad promedio se excede), los paquetes de dicho flujo se eliminarán o se marcarán. Eliminar algunos paquetes reduce la velocidad del flujo y conforma sus parámetros a los valores especificados en el perfil de tráfico. Es necesario marcar los paquetes sin eliminarlos con el fin de garantizar que todos ellos aún son atendidos por el nodo actual (o por sus vecinos) —aunque con parámetros QoS deteriorados diferentes de los que se especificaron en el perfil (por ejemplo, con mayor número de retardos)—.

- **Formateo del tráfico**. Esta función se ha diseñado para el formateo en el tiempo del tráfico que está sujeto a ciertas políticas. Básicamente, dicha función se utiliza para emparejar las ráfagas de tráfico y hacer el flujo de salida más uniforme que el flujo en la entrada al dispositivo. El emparejamiento de las ráfagas ayuda a reducir las colas en los dispositivos de la red que procesarán el tráfico después de un dispositivo determinado. También es conveniente utilizarlo para restablecer las relaciones de tiempo del tráfico de las aplicaciones que trabajan con corrientes, como las aplicaciones de voz.

  Los mecanismos para acondicionar el tráfico pueden estar soportados por cada nodo de la red o estar implementados solamente en los dispositivos de orilla de las redes. Los proveedores de servicios usan con frecuencia esta última variante cuando acondicionan el tráfico de sus clientes.

Existe una diferencia principal en el comportamiento del sistema descrito para garantizar la velocidad de flujo promedio, por un lado, y para garantizar los umbrales requeridos de los retardos y las variaciones en éstos, por el otro.

El valor requerido de la velocidad promedio de servicio se garantiza mediante la configuración del porcentaje de ancho de banda asignado cuando se utilizan las colas ponderadas. Por lo tanto, la red puede realizar la solicitud de cualquier velocidad de flujo promedio, siempre y cuando ésta no exceda el ancho de banda disponible en la red a lo largo de la ruta del flujo en particular.

Sin embargo, la red no puede configurar el algoritmo de colas con prioridad de tal manera que garantice que ésta observará estrictamente el requerimiento de algunos valores de umbral predefinidos del retardo y de la variación de éste. El envío de los paquetes a la cola de prioridades sólo permite garantizar que el número de retardos será lo suficientemente pequeño, al menos mucho menor que el de los paquetes atendidos de acuerdo con el algoritmo de colas ponderadas. Sin embargo, resulta difícil evaluar de manera numérica los retardos. ¿Cómo puede el proveedor del servicio observar el SLA?

Como regla general, este problema se resuelve mediante la medición del tráfico en la red. El proveedor del servicio debe organizar la cola de prioridades para el tráfico, con el uso de una o más colas de prioridad, la medición de los retardos del tráfico en tiempo real y el procesamiento de los resultados con métodos estadísticos. Para lograr esto, el proveedor del servicio debe realizar los histogramas de la distribución de los retardos para las diferentes rutas del flujo y determinar los retardos promedio, las variaciones del retardo y las variaciones máximas del retardo para todas las clases de tráfico sensible al retardo. Con base en estas características, el proveedor del servicio selecciona algunos rasgos QoS de umbral que pueda garantizar a sus clientes. Como regla general, estos valores se seleccionan con algunas reservas, de manera que la red observe las garantías declaradas aun cuando aparezcan algunos clientes nuevos.

7.8 INGENIERÍA DE TRÁFICO

PALABRAS CLAVE: requerimientos QoS, ingeniería de tráfico, perfil de tráfico, clases de tráfico, ráfaga de tráfico, reservación de recursos, rutas de tráfico suboptimizadas, flujos agregados, switches de tránsito, nivel de utilización del recurso, mecanismo para controlar la congestión, y redes de conmutación de paquetes.

Cuando se considera la reservación basada en el sistema QoS, no se cubren aspectos como las rutas a lo largo de las cuales viajan los flujos a través de la red. Para ser más precisos, se estima que estas rutas están predefinidas, una elección que se hizo sin tener en cuenta los requerimientos QoS. En estas condiciones de rutas predefinidas, se trata de asegurar que dicho conjunto de flujos viaje a través de esta ruta para la cual es posible garantizar la conformidad con los requerimientos de QoS.

La tarea de garantizar el soporte QoS podrá resolverse de manera más eficaz si se asume que las rutas de tráfico no son constantes y pueden seleccionarse. Esto permitiría que la red atendiera a número mayor de flujos y garantizaría los requerimientos del QoS, siempre y cuando las características de la red (es decir, el ancho de banda del enlace y el desempeño del switch) no cambiaran.

Los métodos de la ingeniería de tráfico (ET, por sus siglas en inglés) resuelven el problema de la selección de rutas para los flujos (o clases de tráfico) y el cumplimiento de los requisitos del QoS. Dichos métodos tratan de lograr otro objetivo, de modo simultáneo: garantizar una carga balanceada de los recursos de la red que esté lo más cercana al máximo como sea posible. Cuando se alcanza este objetivo, la red tendrá un desempeño general máximo y garantizarán las características de QoS especificadas.

Los métodos de TE también se basan en la reservación de recursos. Además de seleccionar una ruta óptima para el flujo, dichos métodos reservan el ancho de banda de los recursos de la red junto con esta ruta para tal flujo.

Los métodos de TE son relativamente nuevos en las redes de conmutación de paquetes. Básicamente, esto se debe a que la transmisión de tráfico elástico no ejerció gran presión sobre los parámetros QoS. Además, por mucho tiempo, Internet no era una red comercial; por lo tanto, la utilización máxima de los recursos no era un problema de importancia significativa para las tecnologías IP que servían como el fundamento de Internet.

La situación ha cambiado. Las redes de conmutación de paquetes transmiten diferentes tipos de tráfico, proporcionan el QoS especificado y garantizan una utilización máxima de sus recursos; sin embargo, para alcanzar esta meta, es necesario modificar algunos métodos convencionales para la selección de las rutas.

7.8.1 Desventajas de los métodos de enrutamiento convencionales

La selección de rutas con base en la topología de la red que no tiene en cuenta la información acerca de la carga real en ésta fue el principio de operación más importante de los protocolos de enrutamiento en las redes de conmutación de paquetes.

Por cada par dirección de origen-dirección de destino, dichos protocolos seleccionan la única ruta sin tener en cuenta los flujos de información que viajan a través de la red. Como resultado, todos los flujos entre dichos pares de nodos terminales pasan a través de esta ruta,

la más corta de acuerdo con las mediciones de la métrica. La ruta seleccionada puede ser más racional (por ejemplo, que tenga en cuenta el ancho de banda nominal de los enlaces de comunicaciones o las pérdidas introducidas por dichos enlaces) o menos racionales (por ejemplo, que considere solamente el número de ruteadores de tránsito entre los nodos de origen y de destino).

IMPORTANTE *Los métodos de enrutamiento convencionales tienen en cuenta la selección de la mejor ruta como la única posible, incluso si existen otras rutas que sean más largas.*

La red tipo *pescado*, aquella con la topología que se muestra en la figura 7.14, es un ejemplo clásico que ilustra la ineficacia de este método. A pesar de las dos rutas entre los switches A y E —la superior a través del switch B y la inferior a través de los switches C y D—, todo el tráfico desde el switch A hacia el E será enviado a la largo de la ruta superior de acuerdo con los principios del enrutamiento convencional. Esto sucede por una razón: la trayectoria inferior es más larga por un nodo de tránsito. Por lo tanto, se ignora esta ruta a pesar de que puede operar en paralelo con la superior.

En consecuencia, aun la ruta más corta se congestiona y los paquetes se enviarán a través de esta ruta de cualquier forma. Por ejemplo, en la red que se muestra en la figura 7.15, la trayectoria superior seguirá utilizándose aunque sus recursos demuestren ser insuficientes para atender el tráfico desde A hacia E. Al mismo tiempo, la trayectoria inferior será ignorada a pesar de que los recursos de los switches B y C deben ser suficientes para transmitir con alta calidad este tráfico.

La ineficacia de los métodos utilizados para la distribución de los recursos de la red es evidente. Algunos recursos operan en condiciones de sobrecarga, pero otros no se usan. Los métodos para controlar la congestión no pueden resolver este problema, ya que comienzan a manejarla en condiciones de pérdida cuando resulta imposible encontrar una solución racional. Los métodos de reservación tampoco pueden resolver este problema si intentan reservar recursos a través de las rutas seleccionadas sin tener en cuenta la carga actual de los switches de la red. En consecuencia, principalmente son necesarios diversos mecanismos.

7.8.2 Panorama de la ingeniería de tráfico (TE)

Los métodos de la TE utilizan los datos iniciales siguientes:

- Características de la red: su topología, así como el desempeño de sus switches y el ancho de banda de sus enlaces de comunicaciones (figura 7.15).

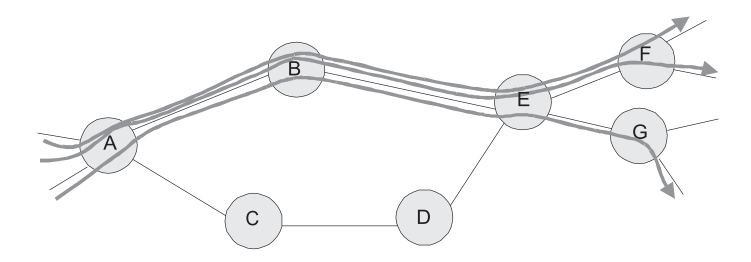


FIGURA 7.14 Ineficacia del método de selección de la ruta más corta.

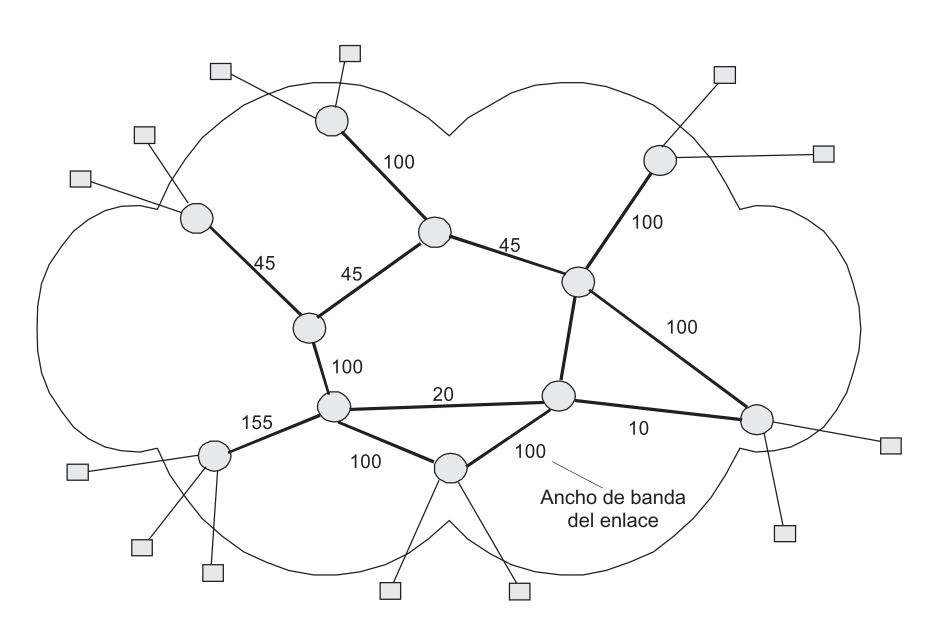


FIGURA 7.15 Topología de la red y desempeño de sus recursos.

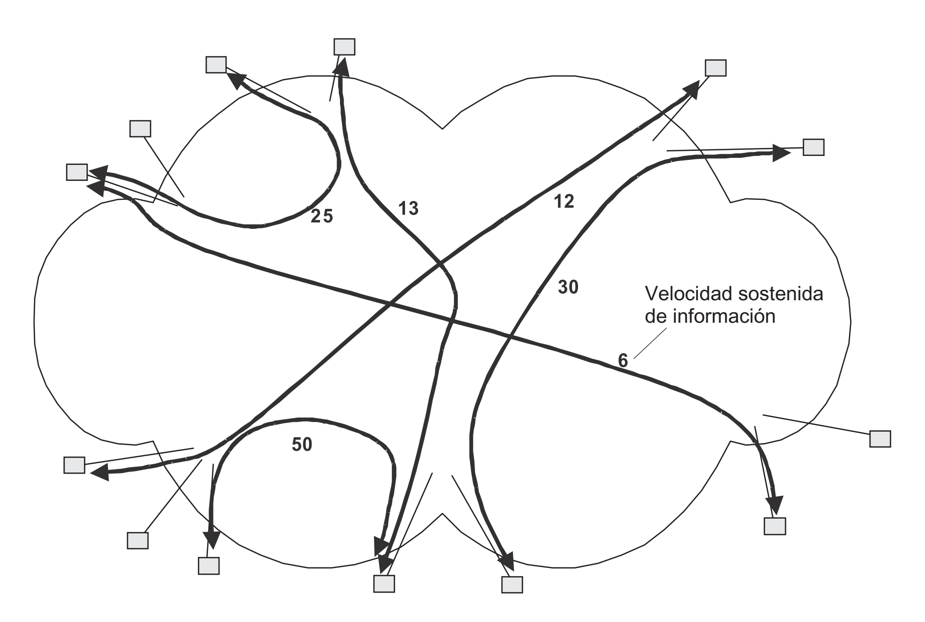


FIGURA 7.16 Carga ofrecida.

- Información acerca de la carga ofrecida, esto es, acerca de los flujos de tráfico que la red debe transmitir entre sus switches de orilla (figura 7.16).

Suponga que el desempeño del procesador de cada switch es suficiente para atender el tráfico de todas sus interfaces de entrada incluso si dicho tráfico llega a la interfaz a la velocidad máxima posible, es decir, a una que sea igual al ancho de banda de la interfaz. Por lo tanto, cuando se lleva a cabo la reservación de recursos, deben considerarse como recursos el ancho de banda de los switches que conectan el enlace, lo cual determina el ancho de banda de las dos interfaces conectadas mediante el enlace.

Cada flujo está caracterizado por el punto de entrada hacia la red, el punto de salida de la red y el perfil de tráfico. Para obtener soluciones óptimas, es posible utilizar descripciones detalladas de cada flujo. Por ejemplo, tenga en cuenta el valor de posibles ráfagas de tráfico o de las variaciones de los intervalos entre paquetes. Sin embargo, como es difícil evaluar cuantitativamente su influencia en la operación de la red y la manera en la que estos parámetros afectan las características QoS es menos importante, para encontrar la distribución subóptima de la rutas de tráfico, por lo general sólo se tienen en cuenta las velocidades de información sostenida de los flujos, los cuales se muestran en la figura 7.17.

Los métodos de TE trabajan con flujos agregados que conectan varios flujos en lugar de hacerlo con flujos individuales. Como buscamos una ruta común para varios flujos, solamente podrán agregarse aquellos que tengan una entrada común a la red y puntos de salida. Agregar flujos simplifica el problema de seleccionar rutas, ya que cuando se considera el flujo individual del usuario, los switches de tránsito tienen que almacenar cantidades excesivas de información debido a que los flujos individuales pueden ser muy numerosos. Sin embargo, es necesario destacar que la agregación de varios flujos individuales es posible sólo cuando los flujos componentes solicitan las mismas demandas respecto al QoS. Con el fin de ser breves, más adelante en esta sección se utilizará el término *flujo* para designar tanto flujos individuales como agregados, ya que esto no modifica los principios de la TE.

> El objetivo de la TE es determinar las rutas para enviar flujos a través de la red, lo cual significa que para cada flujo es necesario encontrar la secuencia exacta de switches de tránsito y sus interfaces. Dichas rutas deben seleccionarse de tal forma que todos los recursos de la red se carguen al máximo y que se garantice que cada flujo tenga el QoS requerido.

El nivel máximo de uso de recursos se selecciona de tal manera que permita que los mecanismos para controlar la congestión garanticen el QoS necesario. Por simplicidad, más adelante se supondrá que la red en estudio transmite sólo una clase de tráfico (por ejemplo,

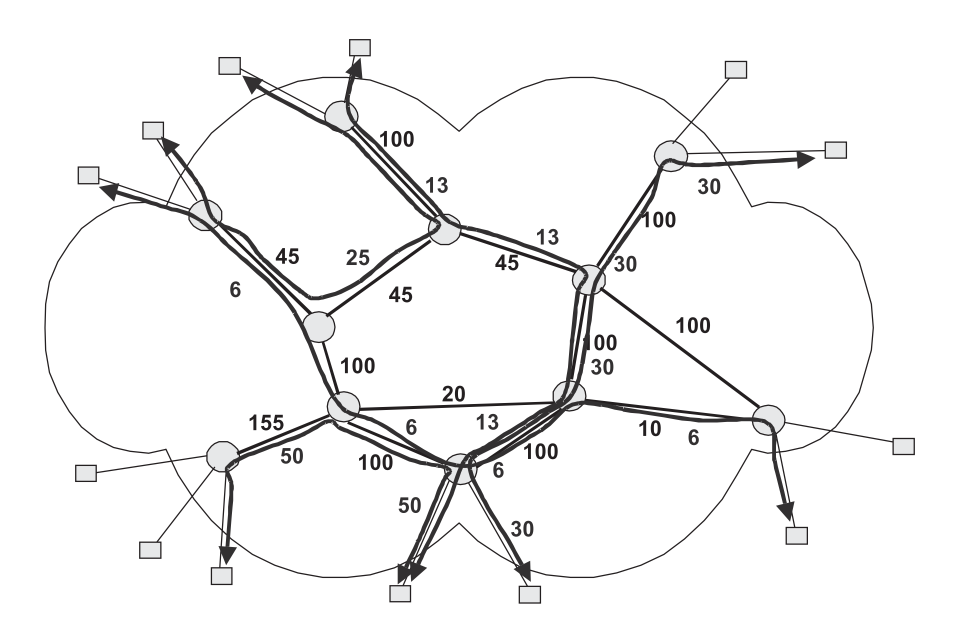


FIGURA 7.17 Distribución de la carga en la red: selección de rutas de tráfico.

tráfico sensible al retardo) y después explicaremos la manera de generalizar métodos de TE cuando la red tenga que transmitir diferentes tipos de tráfico.

La solución del problema de la TE es un conjunto de rutas para un grupo específico de flujos de tráfico para los cuales todos los valores de los coeficientes de utilización de recursos a lo largo de la ruta no excedan un umbral predefinido, $K_{máx}$.

La figura 7.17 muestra una solución posible al problema que se observa en las figuras 7.16 y 7.17. Las rutas seleccionadas garantizan que el coeficiente de utilización máximo de cualquier recurso para cualquier flujo no exceda de 0.6 (es decir, $K_{máx}$ en este ejemplo es de 0.6).

Existen distintos métodos para resolver el problema de la TE. Primero, es posible encontrar una solución con antelación en el modo en segundo plano. Con este propósito, es necesario conocer los datos iniciales: topología y desempeño de la red, así como los puntos de entrada y salida de los flujos de tráfico a la red y sus velocidades promedio. Después de esto, el problema de distribuir racionalmente las rutas entre los flujos de tráfico con puntos de entrada y salida constantes y niveles predefinidos de los coeficientes de utilización máxima puede dejarse a cargo de algún programa. Por ejemplo, dicho programa puede encontrar la solución mediante la prueba de todas las variantes posibles. El resultado de su operación se presentará en la forma de rutas exactas para cada flujo, y se especificarán todos los switches de tránsito.

El segundo método supone que el problema de TE se resolverá si se deja a cargo de los switches de la red. Para este efecto, es posible emplear versiones modificadas de los protocolos de enrutamiento estándares. Las modificaciones introducidas en los protocolos de enrutamiento significan que los switches y ruteadores no solamente se informan uno al otro acerca de los datos topológicos, sino también intercambian los valores actuales del ancho de banda disponible de cada recurso.

Después de encontrar la solución, es necesario implementarla en la forma de tablas de enrutamiento. En esta etapa podrá surgir otro problema si usted necesita establecer estas rutas en una red de datagramas. Las tablas de enrutamiento en dichas redes solamente tienen en cuenta las direcciones de destino de los paquetes. Los switches y ruteadores de dichas redes (por ejemplo, las redes IP) no trabajan con flujos, ya que los flujos individuales no existen de manera explícita. En dichas redes, cada paquete es una unidad de conmutación individual durante el envío. En otras palabras, las tablas de transferencia de dichas redes reflejan solamente la topología de la red (las direcciones de envío a direcciones de destino específicas).

Por lo tanto, infundir métodos de reservación en las redes de datagramas es un proceso con dificultades significativas. Los protocolos de reservación similares al RSVP que ya se mencionó usan conjuntos de características además de la dirección de destino para definir el flujo de los ruteadores de datagramas. En este caso, el concepto de flujo se usa sólo en la etapa de reservación y durante el envío el esquema tradicional sigue trabajando (es decir, el que emplea solamente la dirección de destino).

Ahora imagine que tenemos varios flujos (suponga todavía que todos ellos pertenecen a la única clase de tráfico) entre dos nodos terminales y que deben enviarse a través de rutas diferentes. Dicha situación puede surgir cuando se resuelve el problema de TE que consiste en establecer el balance de la carga de la red. Los switches o ruteadores de datagramas no pueden dar la solución, pues para todos estos flujos solamente se cuenta con un registro en la tabla de enrutamiento, el cual corresponde a la dirección común de destino de los paquetes que pertenecen a estos flujos. El cambio de la lógica de operación de los switches y ruteadores en las redes de datagramas no es una tarea rápida, porque requiere modificaciones fundamentales.

Por lo tanto, en la actualidad se utilizan métodos de la TE en las redes con circuitos virtuales para los que la implementación de la solución obtenida por uno o varios grupos de flujos no presenta ningún problema. Cada flujo (o grupo de flujos con la misma ruta) recibe circuitos virtuales asignados, creados de acuerdo con la ruta seleccionada. Los métodos de TE se emplean con éxito en las redes ATM y Frame Relay que trabajan con base en la técnica de circuitos virtuales. Las redes IP pueden también beneficiarse de las ventajas de la TE cuando se utilizan en redes ATM o Frame Relay que trabajan como parte de una interred diseñada con base en el protocolo IP. Una nueva tecnología, MPLS, se diseñó específicamente como una herramienta para integrar las técnicas de circuitos virtuales con las redes IP. MPLS puede usarse para resolver problemas de TE en las redes IP.

Los métodos de TE para cada tecnología en particular se estudiarán en detalle junto con sus respectivas tecnologías más adelante en este libro.

7.8.3 Ingeniería de tráfico para las distintas clases de tráfico

El problema de la TE que se estudió en la sección anterior se presentó de manera simplificada. Todos los flujos de tráfico pertenecían a la misma clase de tráfico y tenían los mismos requerimientos QoS. Esto permitió que el mismo valor máximo del coeficiente de utilización $K_{máx}$ se empleara para todos los flujos.

Algunas veces para cada usuario de red existen varias clases de tráfico. Ya se ha explicado un problema similar cuando se estudió la reservación de recursos.

Esto significa que es necesario proporcionar un valor, $K_{máx}$, a cada clase de tráfico.

Los métodos de TE que tienen en cuenta la presencia de tráfico con diferentes niveles de requerimientos QoS resuelven este problema de la misma forma que los métodos de reservación de recursos de los nodos individuales. Si tenemos dos clases de tráfico, debemos especificar dos niveles máximos de utilización de recursos. Por ejemplo, para el tráfico elástico, el valor máximo del coeficiente de utilización no debe ser mayor que 0.9, y para el tráfico sensible al retardo, este valor no debe exceder de 0.5. Como regla general, la reservación no se lleva a cabo en todos los flujos, pues parte del ancho de banda debe estar disponible. Por esta razón, los valores máximos proporcionados con anterioridad se reducen a algunos valores alrededor de 0.75 y 0.25, respectivamente.

Para lograr dichos resultados, cada recurso debe tener dos contadores del ancho de banda disponibles: uno para el tráfico con prioridad sensible al retardo y otro para el tráfico elástico. Cuando se determina la posibilidad de diseñar la ruta con el uso de recursos específicos, la velocidad promedio del nuevo flujo para tráfico con prioridad deberá compararse con el ancho de banda disponible para el tráfico con prioridad. Si el ancho de banda disponible es suficiente y el nuevo flujo pasará empleando esta interfaz, la velocidad del nuevo flujo deberá restarse del contador del ancho de banda disponible para tráfico con prioridad, así como del contador del ancho de banda disponible para el tráfico elástico, ya que el tráfico con prioridad siempre se atenderá antes que el elástico. Por lo tanto, el tráfico con prioridad también generará una carga adicional para el tráfico elástico. Si el problema de TE se resuelve para el tráfico elástico, su velocidad se comparará con el contador de ancho de banda disponible para ese mismo tipo de tráfico.

Si se toma una decisión positiva, el valor de esta velocidad deberá restarse sólo del contador del tráfico elástico, ya que el tráfico elástico es transparente para el tráfico con prioridad.

Los protocolos de enrutamiento modificados deben distribuir información a través de la red acerca de dos parámetros de ancho de banda disponibles de forma separada para cada clase de tráfico. Si este problema se generaliza para la transmisión de varias clases de

tráfico, cada recurso deberá tener el mismo número de contadores asociados de acuerdo con el número de clases de tráfico que haya en la red. Los protocolos de enrutamiento deben distribuir el vector con valores de ancho de banda libre que contengan el número apropiado de elementos.

RESUMEN

- La calidad del servicio en un sentido estricto se enfoca en la influencia de las colas de los dispositivos de comunicaciones en la transmisión de tráfico. En la actualidad, los métodos QoS tienen una de las posiciones más importantes en el rango de tecnologías que se utilizan en las redes de conmutación de paquetes. Sin la implementación de estos métodos, la operación de las aplicaciones multimedia actuales (como la telefonía IP, la difusión de video y audio y el aprendizaje remoto interactivo) sería imposible.
- El tráfico de aplicaciones puede dividirse en dos grandes clases en relación con sus requerimientos de características QoS: tráfico sensible al tiempo y tráfico elástico.
- Las características QoS reflejan los efectos negativos de los paquetes que esperan tiempo haciendo cola, lo cual se manifiesta en una reducción de la velocidad de transmisión, en el daño de paquetes y en las pérdidas.
- Las colas con prioridad y las ponderadas, así como la reservación de recursos y la retroalimentación permiten garantizar el QoS para el tráfico sensible al retardo y para el tráfico elástico.
- El algoritmo de ventana deslizante garantiza la transmisión confiable de paquetes y representa una herramienta de retroalimentación confiable.
- La arquitectura de un sistema QoS basado en la reservación incluye:
  - Mecanismos de colas.
  - Protocolos de reservación que permiten reservar de forma automática los recursos requeridos para los flujos.
  - Herramientas para el acondicionamiento de tráfico que llevan a cabo la clasificación, política y formateo del tráfico.
- Los métodos de ingeniería de tráfico consisten en la selección racional de rutas para la transmisión de flujos utilizando la red. Dicha selección maximiza el uso de los recursos de la red y garantiza la conformidad con los requerimientos QoS.

PREGUNTAS DE REPASO

1. Proporcione ejemplos de aplicaciones que generen tráfico elástico.
2. ¿Qué características del QoS son las más importantes para el tráfico sensible al tiempo?
3. ¿Cuáles son los efectos positivos y negativos del uso de colas en los switches de paquetes?
4. ¿Qué parámetro tiene la mayor influencia en el tamaño de las colas? y ¿qué parámetro es el segundo en importancia?
5. ¿Qué tipos de tráfico transmiten las redes de conmutación de paquetes? y ¿cuáles son sus requerimientos para la red?
6. ¿Cuáles son las ventajas y desventajas de las colas con prioridad?
7. ¿Para qué tipo de tráfico es más apropiada la cola ponderada?

8. ¿Es posible combinar las colas con prioridad y las ponderadas?
9. ¿Pueden los paquetes con la prioridad más alta sufrir retardos en las colas?
10. Liste los métodos para controlar y eliminar la congestión.
11. ¿Cuáles son las diferencias entre la reservación de ancho de banda en las redes de conmutación de paquetes y en las de conmutación de circuitos?
12. ¿Cuáles son los componentes del sistema QoS basado en la reservación?
13. ¿Qué problema se resuelve mediante el uso de los métodos de ingeniería de tráfico?
14. ¿Qué parámetro de tráfico se puede cambiar en la ingeniería de tráfico?

PROBLEMAS

1. Suponga que algún flujo de datos pertenece a la clase CBR. Los datos se transmiten en paquetes iguales a 125 bytes a través de un enlace de 100 Mbps. El perfil de tráfico tiene los parámetros siguientes: el PIR para los periodos de ráfagas es de 25 Mbps, la desviación máxima del intervalo entre paquetes es de 10 ms y el periodo de ráfaga es de 600 ms. Si el tráfico está acorde con su perfil, ¿cuál será el volumen máximo de la ráfaga?
2. ¿Cuál de los cinco flujos esperará en promedio menos tiempo en la cola de la interfaz de salida de 100 Mbps si dichos flujos se atienden mediante colas ponderadas y se les asignan el 40, 15, 10, 30 y 5% del ancho de banda de la interfaz, respectivamente? Las velocidades de flujo promedio son 35, 2, 8, 3 y 4 Mbps, respectivamente. El coeficiente de variación de los intervalos entre paquetes es el mismo para todos los flujos.
3. ¿Para cuál de los eventos que se listan aquí el flujo de la cola con la prioridad más alta tiene que esperar en una cola?
   a) Colas con prioridades bajas.
   b) Su propia ráfaga.
   c) Ráfagas de tráfico con baja prioridad.
4. Existen tres colas en la interfaz de salida a 10 Mbps, atendidas de acuerdo con el algoritmo de colas ponderadas. Hay tres paquetes en la primera cola: el paquete 1 es de 1 500 bytes, el 2 es de 625 bytes y el 3 de 750 bytes. En la segunda cola están el paquete 4 (500 bytes), el 5 (1 500 bytes) y el 6 (1 500 bytes). En la tercera cola se hallan el paquete 7 (100 bytes), el 8 (275 bytes), el 9 (1 500 bytes) y el 10 (1 500 bytes). En las colas, los paquetes están en orden ascendente (es decir, el primer paquete en la primera cola es el 1, en la segunda cola está el 4 y en la tercera cola se encuentra el paquete 7).
5. ¿En qué orden aparecerán los paquetes a la salida de la interfaz de 2 Mbps, si el ciclo de trabajo del algoritmo es de 10 mseg y a las colas se les asignan 50, 30 y 20% del ancho de banda del recurso, respectivamente? En cada ciclo, el algoritmo siempre toma un paquete de la cola (siempre y cuando no esté vacía), incluso si el tamaño de paquete garantiza que su transmisión excede el tiempo asignado a esta cola.
6. ¿Cuánto tiempo tomará completar cada uno de los dos ciclos de procesamiento de colas (consulte la pregunta anterior)? y ¿a qué velocidad se atendió cada flujo en este intervalo que comprende dos ciclos?
7. ¿Cómo es necesario cambiar el tiempo del ciclo del algoritmo descrito en la pregunta 4 para hacer las velocidades de flujo más cercanas a las planeadas? ¿Aumentarlo o reducirlo?
8. Al ingresar a la red, un flujo experimenta una política de acuerdo con el perfil de 3 Mbps. A este flujo se le asigna un 30% de los 10 Mbps del ancho de banda de la interfaz de salida en el switch de tránsito de la red. ¿Cuáles aseveraciones son correctas?

a) El resultado de aplicar cualquiera de estos mecanismos es el mismo; por lo tanto, no es necesario implementar reservación en el switch.

b) El resultado de aplicar cualquiera de estos mecanismos es el mismo, pero la reservación en el switch es necesaria debido a que en la entrada a la red y dentro del switch el flujo compite por los recursos con otros flujos.

c) Los resultados que se obtienen al aplicar cualquiera de estos mecanismos son diferentes. A la entrada de la red, la velocidad de flujo está limitada a 3 Mbps; y en el switch de este flujo, la velocidad de 3 Mbps está garantizada aun durante periodos de congestión.

9. ¿Es posible no tener ninguna cola en un sistema cuyo coeficiente de utilización esté cercano a 1?

10. ¿Cuál de los mecanismos que se listan aquí se debe utilizar para garantizar la transmisión con alta calidad de tráfico de voz (flujo de 64 Kbps) si se usa la red de conmutación de paquetes?

a) Reservar un ancho de banda de 64 Kbps de todos los switches a lo largo de la ruta de tráfico de voz.

b) Atender este flujo en la cola con prioridad en todos los switches a lo largo de la ruta de tráfico.

c) Utilizar la memoria de entrada de paquetes del nodo de recepción de la red.

d) Emparejar el tráfico en las colas de salida de todos los switches a lo largo de la ruta.

11. ¿Es correcta la siguiente afirmación? La reservación de recursos en las redes de conmutación de paquetes restringe al usuario la posibilidad de redistribuir dinámicamente el ancho de banda entre flujos.

12. ¿Qué mecanismo debe aplicarse con el fin de evitar la supresión del tráfico de baja prioridad por el de alta prioridad?

PARTE II

TECNOLOGÍAS DE LA CAPA FÍSICA

El fundamento físico de cualquier red de computadoras (o de telecomunicaciones) lo constituyen sus enlaces de transmisión. *Sin dichos enlaces, los switches no podrían intercambiar paquetes y las computadoras serían dispositivos aislados.*

Después de estudiar los principios del diseño de las redes de computadoras, los lectores podrán imaginar una forma sencilla de una red de computadoras —computadoras y switches conectados entre sí con segmentos de cable—. Sin embargo, cuando se estudia con más detalle una red de computadoras, las cosas demuestran ser significativamente más complejas de lo que parecían cuando se analizó el modelo OSI.

Los cables dedicados se utilizan para conectar dispositivos de red a cortas distancias (es decir, en las LAN). Cuando se instalan WAN y MAN, el costo de este método se eleva demasiado y su uso es ineficiente debido al alto costo de los enlaces de transmisión de larga distancia; además, para instalar dichos cables, es necesario obtener un permiso oficial. Por lo tanto, el uso de redes de conmutación de circuitos regionales existentes —ya sea redes telefónicas o redes de transmisión— representa una solución más eficaz para conectar switches WAN y MAN. En consecuencia, en la red de conmutación de circuitos se crea un circuito que lleva a cabo las mismas funciones de la sección de cable, o sea, éste garantiza las conexiones físicas punto a punto. Tal circuito es un sistema técnico significativamente más intrincado que el cable; sin embargo, dichas complejidades son transparentes para las redes de computadoras. Las redes de transmisión están construidas específicamente para crear infraestructura de enlaces de comunicaciones, y hacen que sus enlaces sean más eficaces respecto a la relación precio/capacidad. En la actualidad, los diseñadores de redes de computadoras cuentan con una amplia gama de enlaces de transmisión a su disposición que abarcan velocidades desde 64 Kbps hasta 10 Gbps.

A pesar de las diferencias de la naturaleza física y técnica de los enlaces de comunicaciones, éstos pueden describirse mediante el uso de un conjunto unificado de características. Los parámetros técnicos más importantes de cualquier enlace de comunicaciones que transmite información discreta son su ancho de banda, medido en Hertz, y su capacidad, medida en bits por segundo (bps). La capacidad es la velocidad máxima de la corriente de bits que puede lograrse en un enlace de comunicaciones determinado. La capacidad depende del ancho de banda y del método utilizado para codificar información discreta.

Los enlaces inalámbricos ganan cada vez más popularidad: son el único tipo de enlace que garantiza la movilidad de los usuarios de una red de computadoras; además, las comunicaciones inalámbricas se utilizan cuando la instalación de cables no es factible o resulta en una operación muy costosa. Esto puede observarse en regiones poco pobladas, en edificios con infraestructura de cableado existente instalada por los competidores, etc. Las comunicaciones inalámbricas usan ondas electromagnéticas a diferentes frecuencias: ondas de radio, microondas, ondas infrarrojas o luz visible. Los elevados niveles de ruido y las complejas trayectorias de propagación típicas de los enlaces inalámbricos requieren emplear métodos especiales de codificación y transmisión de señales.

La parte II está constituida por los capítulos siguientes:

- Capítulo 8: Enlaces de transmisión
- Capítulo 9: Codificación y multiplexaje de datos
- Capítulo 10: Transmisión inalámbrica
- Capítulo 11: Redes de transmisión

8 ENLACES DE TRANSMISIÓN

DESCRIPCIÓN DEL CAPÍTULO

8.1 INTRODUCCIÓN

Cuando se instalan redes, es posible emplear varios enlaces de comunicaciones con el uso de medios físicos diferentes: cables telefónicos y telegráficos colgados entre postes, cables coaxiales y fibra óptica instalados bajo tierra, pares de par trenzado de cobre que conectan todas las oficinas actuales y, por último, ondas de radio que penetran todo.

En este capítulo se analizarán las características generales de los enlaces de comunicaciones independientemente de su naturaleza física. Algunos ejemplos de ellas son el ancho de banda, la capacidad, la probabilidad de error y la inmunidad al ruido. El ancho de banda es una característica fundamental de un enlace de comunicaciones, ya que determina la máxima velocidad de transmisión de información posible del enlace, conocida como *capacidad del enlace*. La **fórmula de Nyquist** expresa esta dependencia para el caso de un enlace ideal, mientras que la **fórmula de Shannon** toma en cuenta la interferencia del ruido siempre presente en los enlaces de comunicaciones reales. Este capítulo concluirá con una descripción de los estándares de cableado actuales, que forman las bases de los enlaces guiados de comunicaciones.

8.2 TAXONOMÍA

PALABRAS CLAVE: enlace, circuito, canal, línea, enlaces de transmisión, red de transmisión, red telefónica, medio físico, par trenzado sin protección (UTP), par trenzado con protección (STP), cable coaxial, cable de fibra óptica, canales de radio, comunicaciones satelitales, amplificador, regenerador, equipo de terminación de circuitos de datos (DCE), unidad de servicios de datos/unidad de servicios de circuitos (DSU/CSU), equipo terminal de datos (DTE), multiplexor, demultiplexor, enlaces analógicos y digitales.

8.2.1 Redes de transmisión, circuitos y enlaces

Cuando se describe técnicamente un sistema que transmite información entre dos nodos de red contiguos, se puede hablar de cuatro términos: **enlace**, **circuito**, **canal** y **línea**. Estos términos se utilizan a menudo como sinónimos y en muchos sentidos esto no es ningún problema. Al mismo tiempo, su uso tiene algunas características específicas.

- El término *enlace* se utiliza para designar al segmento entre dos nodos vecinos. Esto significa que el enlace no incluye la conmutación ni los dispositivos de multiplexaje.
- El término *canal* se usa con mucha frecuencia para designar la parte del ancho de banda del enlace que se utiliza independientemente de los demás canales. Por ejemplo, un circuito en una red de transmisión puede constar de 30 canales, cada uno de los cuales puede tener un ancho de banda de 64 Kbps.
- Un *circuito* es una trayectoria compleja entre los nodos terminales de la red. Por lo tanto, los circuitos están formados por los enlaces individuales y las conexiones internas dentro de los switches.
- Por último, el término *línea* puede emplearse como sinónimo de los tres términos anteriores.

Sin embargo, es necesario comprender que existen varios convencionalismos debido a los cuales las confusiones acerca del uso de los términos no deben juzgarse con mucha severidad.

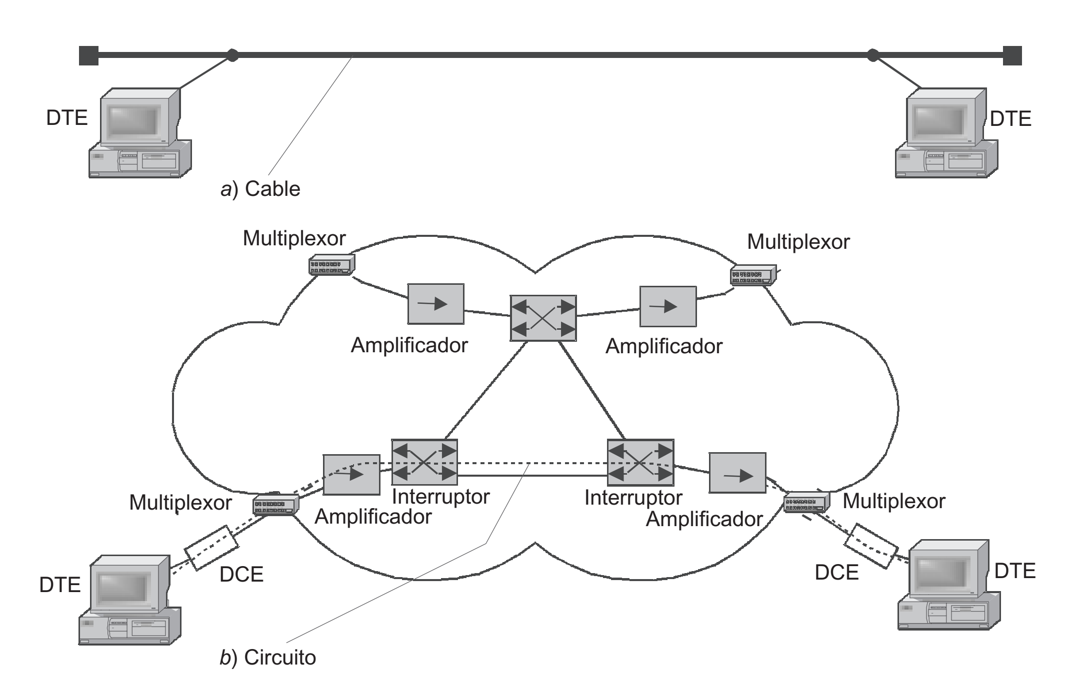


FIGURA 8.1 Componentes de un enlace de comunicaciones.

Esto es especialmente válido respecto a las diferencias en cuanto a terminología entre la telefonía convencional y un área tecnológica nueva: las redes de computadoras. El proceso de convergencia solamente ha agudizado los problemas en cuanto a terminología. Esto sucedió debido a que muchos mecanismos de estas redes se hicieron comunes a ambos tipos de redes, pero conservan dos (o, a veces, más) nombres de cada una de las áreas tecnológicas.

Además de ello, existen razones objetivas para la interpretación ambigua de términos acerca de la conectividad de redes. La figura 8.1 muestra dos variantes de una línea de transmisión. En la primera (figura 8.1*a*), la línea tiene una longitud de decenas de metros de cable. En la segunda (figura 8.1*b*) la línea de transmisión es un circuito establecido en una red de conmutación de circuitos. Esto puede considerarse una **red de transmisión** o una **red telefónica.**

Considérese el caso en el que dos switches de dos redes de computadoras están conectados mediante un enlace de comunicaciones creado dentro de una red de transmisión. Para las redes de computadoras, esta conexión es un enlace, ya que conecta dos nodos vecinos mientras que todo el equipo intermedio es transparente a dichos nodos. Sin embargo, para las redes de transmisión, esta conexión es un circuito —o, para ser más precisos, un canal— pues probablemente utilice parte del ancho de banda de cada enlace que conecta a los switches de la red de transmisión. Por lo tanto, esto se presta para que haya una mala interpretación, a nivel de terminología, entre los especialistas en el campo de las redes de computadoras y los especialistas en el campo de las redes de transmisión. Obsérvese que una red telefónica por sí misma puede estar construida con base en los enlaces de una red de transmisión. Las redes de transmisión se construyen con el fin de proporcionar servicios de transporte a las redes de computadoras o telefónicas. En dichos casos, se puede decir que las redes de computadoras o telefónicas operan a través de redes de transmisión.

8.2.2 Medio de transmisión

Los enlaces de transmisión también son diferentes en cuanto al medio físico que utilicen para transmitir información.

Un **medio fisco de transmisión** que se usa para transmitir datos puede ser un conjunto de alambres a través de los cuales se transmiten señales. Las líneas de comunicaciones de alambre abierto y de cable (subterráneo o sumergido) se construyen con base en estos cables (figura 8.2). Las señales con información pueden también propagarse en otros medios de transmisión, como la atmósfera terrestre o el espacio. En el primer caso se tiene un *medio alámbrico* (*guiado*), mientras que en el segundo se tiene uno *inalámbrico* (*no guiado*).

En los sistemas de comunicaciones actuales, la información se transmite mediante el uso de señales de corriente eléctrica o de voltaje, señales de radio o de luz. Estos procesos físicos son oscilaciones de campos electromagnéticos de diferentes frecuencias.

Las líneas de comunicaciones con *cable abierto* (aéreo) son alambres sin aislante o protección instalados en la parte superior de los postes de potencia. Dichas líneas de comunicaciones fueron las más comunes para la transmisión de señales telefónicas y telegráficas hasta hace poco. En la actualidad, dichas líneas alámbricas aéreas están siendo desplazadas por línea cableadas; sin embargo, pueden todavía utilizarse para transmitir datos de computadora en el caso de no tener disponibles líneas más avanzadas de comunicaciones. La velocidad de transmisión y la inmunidad al ruido de estas líneas están muy lejos de ser perfectas.

Las *líneas cableadas* cuentan con un diseño más complejo. El cable consiste en alambres encerrados en varias capas de protección aislante: eléctrica, electromagnética, mecánica y, posiblemente, climática. El cable también puede estar equipado con conectores que permitan llevar a cabo conexiones rápidas entre los diferentes dispositivos. Los tres tipos de cable siguientes se utilizan en las redes de computadoras (y de telecomunicaciones):

- **Par trenzado sin protección** (UTP) y par trenzado con protección (STP).
- **Cables coaxiales** con protección de cobre.
- **Cables de fibra óptica**.

Los dos primeros tipos de cable se conocen como cable de cobre.

Los **canales de radio de las comunicaciones terrestres y satelitales** están formados por un transmisor y un receptor de ondas de radio. Existe un gran número de canales de radio que difieren en frecuencia y alcance. Los rangos de la difusión de radio (onda larga, onda media y onda corta, también conocida como modulación de amplitud o AM) garantizan comunicaciones de largo alcance a velocidades bajas de transmisión. Los canales que operan

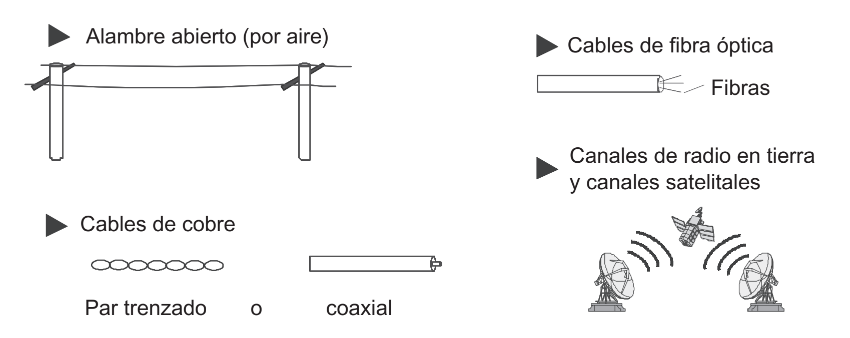


FIGURA 8.2 Tipos de medios de transmisión.

dentro del rango de las altas frecuencias, en el que se utiliza la modulación de frecuencia (FM), proporcionan velocidades más elevadas. Otros rangos de frecuencia, conocidos como ultra-alta frecuencia o microondas (arriba de los 300 MHz), se usan también para transmitir datos. Las señales con frecuencia por arriba de 30 MHz no se reflejan en la ionosfera de la Tierra; por lo tanto, para garantizar una comunicación estable, tanto el transmisor como el receptor deben estar ubicados a la vista. Dichas frecuencias se utilizan en canales satelitales y de radio, así como en las redes de área local y en las redes móviles, donde se satisface esta condición.

En la actualidad, prácticamente todos los tipos de medios de transmisión descritos se emplean para las comunicaciones de datos en las redes de computadoras. La fibra óptica ofrece muchas bondades debido a su gran ancho de banda y alta inmunidad al ruido. Por lo tanto, los cables de fibra óptica se utilizan para construir las troncales de las redes regionales de gran tamaño y de las MAN, así como las LAN de alta velocidad. El par trenzado es otro medio de transmisión muy popular, ya que se caracteriza por tener una relación costo/calidad excelente, así como por su facilidad de instalación. Los canales inalámbricos se usan con mucha frecuencia cuando resulta imposible utilizar enlaces de cable. Por ejemplo, si el canal pasa a través de una región escasamente poblada o es necesario comunicarse con usuarios móviles, se emplean canales inalámbricos. El aseguramiento de la movilidad ha afectado las redes telefónicas, en tanto que las redes de computadoras no pueden todavía alcanzarlas en este sentido. Sin embargo, la instalación de redes de computadoras con base en tecnologías inalámbricas como Radio Ethernet se considera una de las más promisorias áreas tecnológicas de las telecomunicaciones. En el capítulo 10 se estudian con más detalle los enlaces inalámbricos.

8.2.3 Equipo de transmisión

Como se muestra en la figura 8.1, además de los medios de transmisión, las líneas de transmisión incluyen ciertos equipos. Incluso cuando la línea de transmisión no pase a través de redes de este tipo, pero sea creada con base en cables, dicha línea consistirá en un equipo para la **terminación de los circuitos de datos** (**DCE**).

El DCE en una red de computadoras conecta directamente las computadoras de los switches con enlaces de comunicaciones y los convierte en equipo terminal. Tradicionalmente, el DCE está incluido en el enlace de comunicaciones. La lista de los dispositivos DCE incluye **módems** (para las líneas telefónicas), **adaptadores de terminal en redes ISDN** y **dispositivos para la conexión hacia enlaces digitales** de unidades de servicio de datos/unidades de servicio de circuitos (DSU/CSU) de las redes de transmisión.

El DCE trabaja en la capa física del modelo OSI y es responsable de transmitir y recibir señales del tamaño, potencia y frecuencia que se requiera hacia y desde un medio físico.

El equipo del usuario que genera los datos para su transmisión utilizando enlaces de comunicaciones conectados directamente al DCE tiene un nombre generalizado: **equipo terminal de datos** (DTE). Las computadoras, los switches o los ruteadores son ejemplos de DTE. Este equipo no está incluido en las líneas de comunicaciones.

NOTA *No siempre es posible delimitar estrictamente el DTE y el DCE en las LAN. Por ejemplo, un adaptador de LAN puede considerarse parte de una computadora (es decir, el DTE) y parte del enlace de comunicaciones (es decir, el DCE). Para ser más precisos, una parte del adaptador de red lleva a cabo las funciones de DTE; otra parte (la que directamente recibe y transmite las señales hacia y desde la línea) lleva a cabo las funciones del DCE.*

Existen varias *interfaces estándar* para conectar dispositivos DCE a dispositivos DTE (es decir, hacia computadoras, switches y ruteadores).[1] Todos ellos trabajan en distancias cortas, por lo general algunos metros solamente.

El **equipo intermedio** se utiliza generalmente en enlaces de comunicaciones de larga distancia y lleva a cabo las siguientes tareas:

- Mejoramiento de la calidad de las señales.
- Creación de un circuito de comunicaciones persistente entre dos suscriptores de la red

En las LAN puede ocurrir que no exista equipo intermedio dada la longitud del medio físico —cables o señales de radio—, lo cual permite que un adaptador reciba señales directamente de otro sin necesidad de amplificación. Si éste no es el caso, se deben utilizar dispositivos intermedios tales como *repetidores* o *concentradores* (hubs).

En las WAN es necesario garantizar la transmisión de señales de alta calidad a través de cientos o aun miles de kilómetros. Debido a esto, es imposible construir líneas de comunicación de larga distancia sin **amplificadores** (los cuales aumentan la potencia de las señales) y **regeneradores** (los cuales amplifican y restablecen la forma de las señales distorsionadas durante las transmisiones de larga distancia). En general, dichos dispositivos están instalados a una distancia específica predefinida.

En las redes de transmisión, además del equipo considerado anteriormente, el cual garantiza la transmisión de señales con alta calidad, se requiere también equipo de conmutación: **multiplexores**, **demultiplexores** y **switches**. Este equipo forma el circuito continuo construido a partir de las secciones del medio físico (cables con amplificadores) entre dos suscriptores de la red.

En función del tipo de equipo intermedio, todos los enlaces de comunicaciones se dividen en enlaces analógicos y digitales. En los **enlaces analógicos** (o **canales analógicos**), el equipo intermedio está diseñado para amplificar señales analógicas (es decir, señales con un rango continuo de valores). Dichos enlaces se utilizaron tradicionalmente en redes telefónicas para interconectar switches telefónicos. Con la finalidad de obtener canales de alta velocidad que multiplexaran varios loops locales de baja velocidad, se diseñó la técnica *multiplexaje por división de frecuencia* (FDM).

En las **líneas digitales**, las señales que se transmiten tienen un número finito de estados. Como regla, la señal base —es decir, la señal transmitida por ciclo de reloj del dispositivo transmisor— tiene dos, tres o cuatro estados, los cuales se transmiten a través de líneas de comunicaciones como pulsos rectangulares o como voltajes. Tanto los datos de computadora como la voz y el video digitalizado se transmiten con el formato de dichas señales. De hecho, las redes de transmisión son una realidad, debido a la representación discreta y unificada de la información en las redes de computadoras, en las de telefonía y de televisión actuales. En los enlaces de comunicaciones digitales se utiliza equipo intermedio. Los regeneradores mejoran el tamaño de los pulsos y garantizan su resincronización (es decir, restablecen el periodo entre pulsos). El equipo intermedio de multiplexaje y conmutación de las redes de transmisión opera de acuerdo con el principio llamado *multiplexaje por división de tiempo* (TDM).

---

[1] Las interfaces DTE-DCE están descritas por los estándares de la serie V del ITU-T y por las series de Estándares Recomendados (RS) de la EIA. Estas dos líneas de estándares están duplicadas en muchos respectos. Los estándares más populares son el RS-232, el RS-530, el V.35 y el HSSI.

8.3 CARACTERÍSTICAS DE LOS ENLACES DE TRANSMISIÓN

PALABRAS CLAVE: armónica, espectro de las señales, ancho espectral, ruidos externos e internos, atenuación, atenuación lineal, ventanas transparentes, impedancia, umbral de sensibilidad del receptor, inmunidad al ruido, acoplamiento eléctrico, acoplamiento magnético, señales con interferencia, señales con interferencia en el extremo cercano (NEXT), señales con interferencia en el extremo lejano (FEXT), protección de cables, relación entre atenuación y las señales con interferencia (ACR), confiabilidad en la transmisión de datos, tasa de errores (BER), ancho de banda, capacidad, bauds, señal portadora, frecuencia de la portadora, modulación, fórmula de Fourier, Claude Shannon y Harry Nyquist.

8.3.1 Análisis espectral de señales en los enlaces de comunicaciones

La distribución espectral de la señal transmitida a través de enlaces de comunicaciones desempeña un papel muy importante en la determinación de los parámetros de dicha línea. *A partir de la teoría del análisis armónico, se sabe que cualquier proceso periódico puede representarse como la suma de oscilaciones senoidales de frecuencias y amplitudes diferentes* (figura 8.3).

Cada curva senoidal componente se conoce como **armónica** y el conjunto de armónicas se denomina **espectro de la señal.** El **ancho espectral** se interpreta como la diferencia entre las frecuencias máxima y mínima del conjunto de armónicas, cuya suma produce la señal fuente.

Las señales no periódicas pueden representarse mediante señales senoidales integrales con un espectro de frecuencia continuo. En particular, el espectro de un pulso ideal (potencia unitaria y duración cero) contiene las componentes del espectro total de frecuencia, desde $-\infty$ hasta $+\infty$ (figura 8.4).

La técnica para encontrar el espectro de cualquier señal fuente es bien conocida. Para algunas señales que pueden describirse analíticamente (por ejemplo, para la secuencia de pulsos rectangulares con la misma duración y amplitud), el espectro se calcula fácilmente con base en la **fórmula de Fourier.**

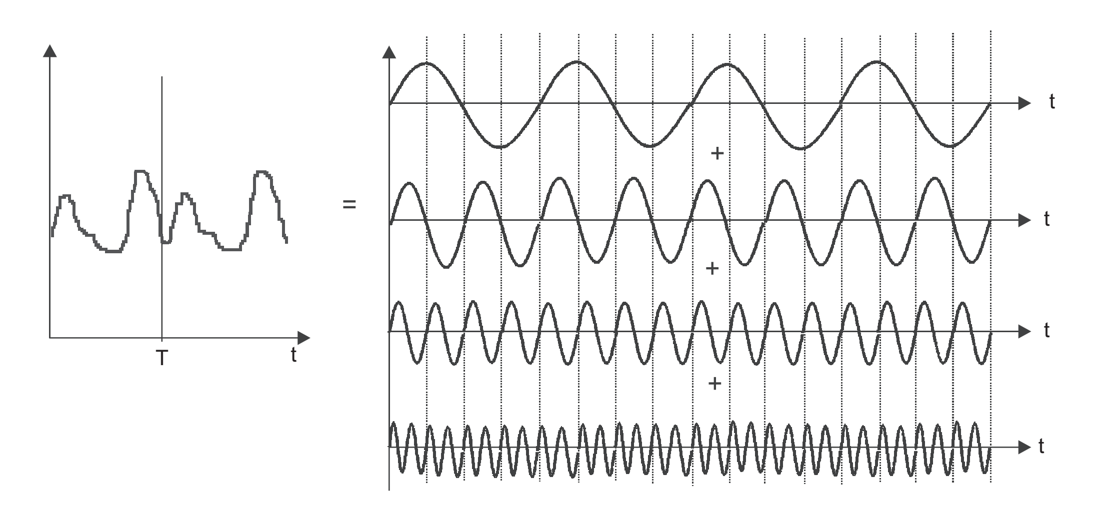


FIGURA 8.3 Representación de una señal periódica mediante la suma de curvas senoidales.

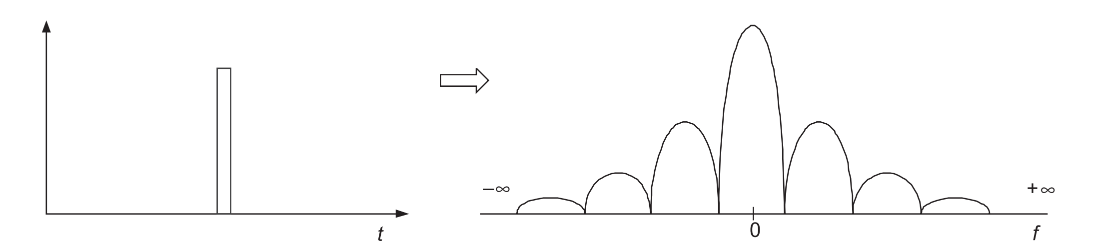


FIGURA 8.4 Espectro de un pulso ideal.

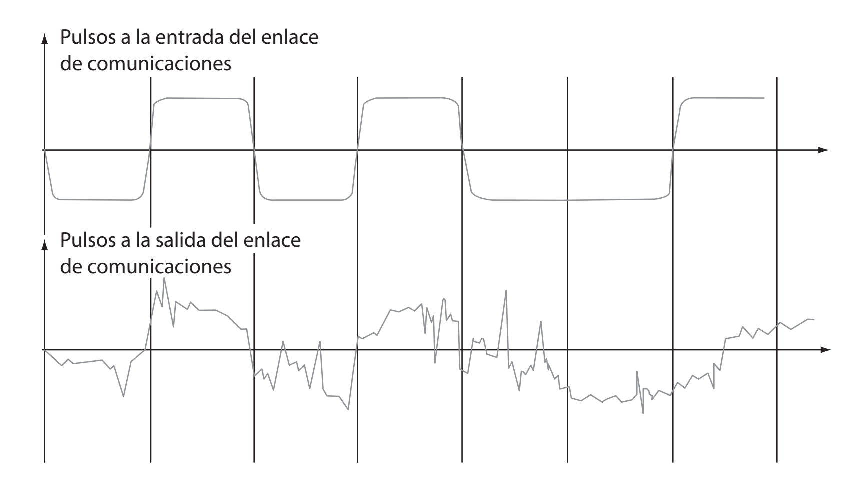


FIGURA 8.5 Distorsión de pulsos en un enlace de comunicaciones.

Para señales que tienen una forma arbitraria, el espectro se podrá encontrar si se utilizan dispositivos especiales conocidos como analizadores de espectros, los cuales miden el espectro de señales reales y despliegan las amplitudes de las componentes armónicas en una pantalla, las imprimen o las transmiten para su procesamiento y almacenamiento en computadoras.

La distorsión de cualquier curva senoidal componente a cualquier frecuencia por la línea de comunicaciones distorsiona la amplitud y la forma de cualquier tipo de señal transmitida. Las distorsiones de forma aparecen cuando las curvas senoidales de diferentes frecuencias se distorsionan de manera distinta. Si se trata de una señal analógica que transmite voz, el timbre de ésta cambia debido a la distorsión de los sobretonos o frecuencias laterales. Cuando se transmiten señales de pulsos característicos de las redes de computadoras, se distorsionan las armónicas de alta y baja frecuencia y, como resultado, los frentes de pulso pierden su forma rectangular (figura 8.5). Por ende, pueden presentarse problemas en el reconocimiento de las señales en el extremo de recepción de la línea.

Las líneas de comunicaciones distorsionan las señales que se transmiten debido a que sus parámetros físicos difieren de los ideales. Un medio de transmisión ideal que no introduzca distorsiones en la señal que se transmite debe, al menos, tener una resistencia, capacitancia e inductancia iguales a cero. Por ejemplo, los pares de cobre son siempre una combinación de cargas resistivas, capacitivas e inductivas activas (figura 8.6). Como resultado, para senoides de diferentes frecuencias, los enlaces tendrán distintos valores de impedancia. En consecuencia, dichas senoides se transmitirán de manera diversa.

Además de distorsiones en las señales introducidas por los parámetros físicos internos del enlace de comunicaciones, existen **ruidos externos** que contribuyen a la distorsión de

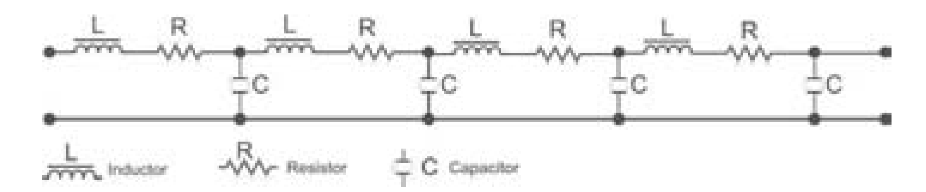


FIGURA 8.6 Representación de un enlace de comunicaciones como una inductancia distribuida y una carga capacitiva.

la forma de la señal a la salida de los enlaces de comunicaciones. Dicho ruido es generado por diferentes máquinas eléctricas, dispositivos electrónicos, fenómenos atmosféricos, etc. A pesar de las medidas de protección tomadas por los diseñadores de cable y la presencia de equipo de amplificación y regeneración, es imposible compensar completamente la influencia del ruido externo. Además de éste, existe **ruido interno** en el cable conocido como interferencia, que es causado por la influencia de un par de alambres en otro. Como resultado, las señales a la salida del enlace generalmente adquieren una forma complicada (como la que se muestra en la figura 8.5).

8.3.2 Atenuación e impedancia

El grado de distorsión de las señales senoidales de los enlaces de comunicaciones se evalúa mediante el uso de características tales como la atenuación y la impedancia.

La **atenuación** muestra cómo la potencia de la señal senoidal de referencia disminuye a la salida del enlace de comunicaciones cuando se compara con la potencia de la señal de referencia proporcionada a la entrada de dicha línea. La atenuación (A) se mide generalmente en decibeles y se calcula de acuerdo con la fórmula siguiente:

$$A = 10\ lg\ P_{sal}/P_{ent} \tag{8.1}$$

Aquí, P_{sal} es la potencia de la señal a la salida de la línea y P_{ent} es la potencia de la señal proporcionada a la entrada de la línea. Como la atenuación depende de la longitud de los enlaces de comunicaciones, la llamada **atenuación lineal** se usa como característica del enlace (es decir, la atenuación de enlaces de comunicaciones de longitudes específicas). Para el cable de una LAN se utiliza generalmente un enlace de 100 m. Este valor es la longitud máxima del cable de la mayoría de las tecnologías de LAN. Para enlaces WAN, la atenuación lineal es de 1 km.

En general, la atenuación caracteriza a las secciones pasivas de los enlaces de comunicaciones, que consisten en cables y conexiones sin amplificadores y regeneradores. Como la potencia de la señal de salida en el cable sin amplificadores intermedios es siempre menor que la potencia de la señal de entrada, la atenuación en el cable tiene siempre un *valor negativo.*

El grado de atenuación de potencia de una señal senoidal depende de la frecuencia senoidal; dicha dependencia se utiliza también para caracterizar los enlaces de comunicaciones (figura 8.7).

Muy a menudo se proporcionan los valores de atenuación para *algunas frecuencias sólo* cuando se describen los parámetros de los enlaces de comunicaciones. El uso de algunos valores solamente y no de todas las características está relacionado, por un lado, con la simplificación de las mediciones cuando se prueba la calidad de la línea y, por otro, con la frecuencia principal de la señal transmitida, a menudo conocida con antelación. Ésta es la

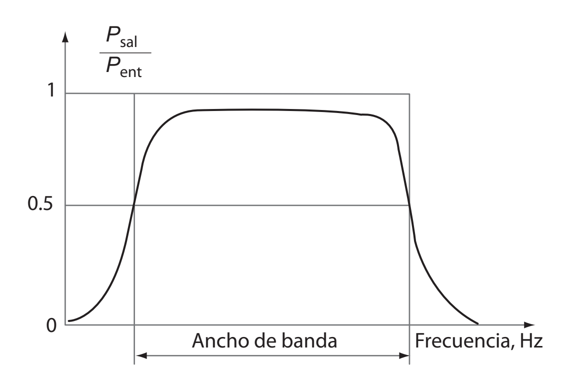


FIGURA 8.7 Dependencia de la atenuación con la frecuencia.

frecuencia cuya armónica tiene la amplitud y potencia más grande. Por lo tanto, a veces es suficiente conocer la atenuación a esta frecuencia, para evaluar, *grosso modo*, las distorsiones de las señales transmitidas a través de la línea.

NOTA *Como ya se mencionó, la atenuación del cable es siempre un valor negativo; sin embargo, los especialistas a menudo omiten el signo de "menos" cuando se refieren a la atenuación. Dichas personas suelen decir que a medida que la calidad de la línea es mejor, su atenuación es menor. Esta afirmación sería correcta solamente si se refiriera al valor absoluto de la atenuación. Si se toma en cuenta el signo, a medida que la atenuación fuese mayor, la calidad del enlace de comunicaciones sería mejor. Veamos un ejemplo: para un cableado en interiores, se utiliza el cable de par trenzado de categoría 5, prácticamente en todas las tecnologías de LAN; además, se caracteriza por tener una atenuación no menor que −23.6 dB a una frecuencia de 100 MHz y una longitud de cable de 100 metros. El cable de categoría 6 de mejor calidad que opera a 100 MHz está caracterizado por una atenuación no menor que a −20.6 dB. Naturalmente, −20.6 > −23.6, pero, al mismo tiempo, 20.6 < 23.6.*

La dependencia típica de la atenuación con respecto a la frecuencia para el par trenzado sin protección (categorías 5 y 6) se muestra en la figura 8.8.

El cable de fibra óptica tiene coeficientes de atenuación significativamente menores (en valor absoluto), que van de –0.2 a –3.0 dB en 1 000 metros de cable. En consecuencia, su calidad es significativamente mayor que la del cable de par trenzado. Prácticamente todas las fibras ópticas tienen una dependencia compleja de la atenuación con la longitud de onda, la cual tiene tres **ventanas de transmisión.** La figura 8.9 muestra la dependencia típica de la atenuación de una fibra óptica. A partir de esta figura, es evidente que el área de aplicación eficaz de las fibras ópticas actuales está en las longitudes de onda de 850 nm, 1 300 nm y 1 550 nm (o en las frecuencias de 35 THz, 23 THz y 19.4 THz, respectivamente). La ventana de 1 550 nm garantiza la obtención de menores pérdidas y, por ende, se puede transmitir a distancias mayores, para un valor constante de potencia de transmisión y sensibilidad del receptor.

Los niveles de potencia absoluta y relativa se utilizan como características de potencia de la señal. El **nivel de potencia absoluta** se mide en watts, mientras que *el **nivel de potencia relativa**, de manera similar a la atenuación, se mide en decibeles*. Al mismo tiempo, 1 mW se considera el valor de referencia con respecto al cual se mide la potencia de la señal. Por lo tanto, el nivel de potencia relativa *p* se calcula de acuerdo con la fórmula siguiente:

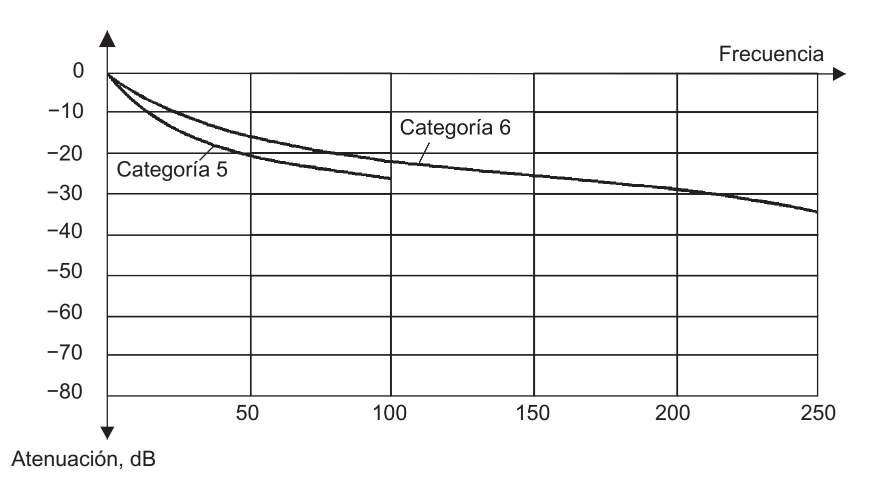


FIGURA 8.8 Atenuación de los cables de par trenzado sin protección.

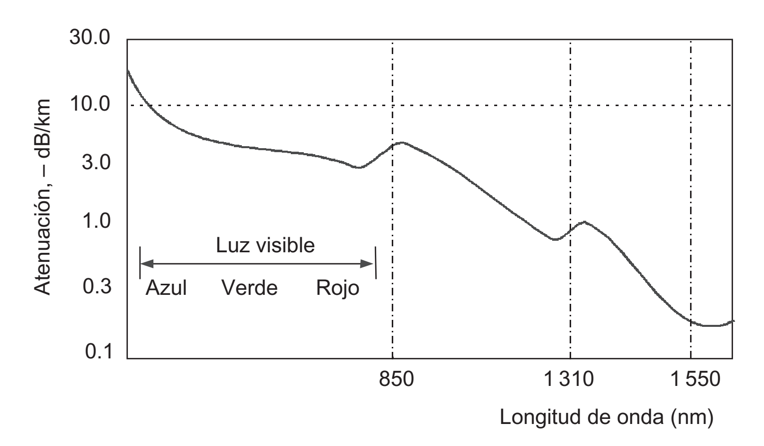


FIGURA 8.9 Ventanas de transparencia de la fibra óptica.

$$p = 10\ lg\ P/1mW[dBm] \qquad (8.2)$$

Aquí p es la potencia absoluta de las señales en miliwatts y dBm es una unidad de medida del nivel de potencia relativa (decibeles por miliwatt).

El uso de los valores de potencia relativa es apropiado cuando se calcula el presupuesto de potencia de los enlaces de transmisión.

EJEMPLO *Suponga que es necesario determinar la potencia relativa mínima* x *(dBm) del transmisor; para ello, es suficiente garantizar que la potencia relativa de la señal de salida no es menor que el valor de umbral* y *(dBm). La atenuación en la línea se conoce y es igual a A. Suponga que X y Y son valores absolutos especificados en mW de la potencia de la señal a la entrada y a la salida de la línea, respectivamente.*
Por definición:

$$A = 10 \log X/Y$$

Mediante el uso de las propiedades de los logaritmos:

$$A = 10 \log X - 10 \lg Y = 10 \log X/1\text{mW} - 10 \lg Y/1 \text{ mW}$$

Observe que al menos dos términos en esta ecuación representan las potencias relativas de la señal a la entrada y a la salida de la línea. Esto produce la relación siguiente:

$$A = x - y$$

A partir de esto, se puede deducir que la potencia mínima del transmisor puede definirse como la suma de la atenuación y la potencia de la señal de salida:

$$x = A + y$$

El cálculo es sencillo debido a que utiliza potencias relativas de las señales de entrada y de salida como datos iniciales.

El valor y *se conoce como **umbral de sensibilidad del receptor,** que es la potencia mínima de la señal a la entrada del receptor a la cual éste puede reconocer perfectamente la información discreta contenida en la señal. Para una operación precisa del enlace de comunicaciones, es necesario garantizar que la potencia mínima de la señal en el transmisor, atenuada por el desvanecimiento del enlace de comunicaciones, excede el umbral de sensibilidad del receptor: $x - A > y$. La verificación de esta condición es la idea primordial en la que se apoya el cálculo del presupuesto de potencia del enlace de transmisión.*

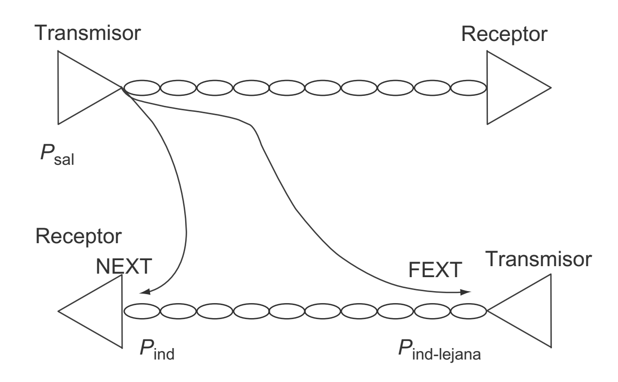
Otro parámetro importante del enlace de comunicaciones de cobre es la **impedancia**. Dicho parámetro es la resistencia total (compleja) a la propagación de ondas electromagnéticas de frecuencias específicas en el circuito. La impedancia se mide en ohms y depende de algunos parámetros de la línea como la resistencia activa, la inductancia lineal y la capacitancia lineal, así como de la frecuencia de la señal. La resistencia de salida del transmisor debe estar relacionada con la impedancia de la línea; de otra forma, el valor de la atenuación de la señal será excesivo.

8.3.3 Inmunidad al ruido y confiabilidad de la transmisión

La **inmunidad al ruido de la línea**, *como su nombre lo indica, determina la capacidad que tiene la línea para soportar la influencia del ruido generado en el medio ambiente o en los conductores internos del mismo cable.* Dicha inmunidad depende del tipo de medio físico de transmisión que se utilice y de las propiedades de la línea en cuanto a la protección y supresión de ruidos. Los canales de radio son los menos resistentes al ruido. Las líneas de pares de cobre son más inmunes al ruido y los cables de fibra óptica tienen la mejor inmunidad al ruido, pues son resistentes a la radiación electromagnética externa. En general, para reducir el ruido que se presenta como resultado de los campos electromagnéticos externos, es necesario utilizar conductores con protección o trenzados.

Los acoplamientos eléctrico y magnético también son parámetros del cable de cobre que caracterizan la influencia del ruido. El **acoplamiento eléctrico** se determina como el cociente de la corriente inducida en el circuito afectado y el voltaje del circuito al que afecta. El **acoplamiento magnético** es el cociente de la fuerza electromotriz inducida en el circuito afectado y la corriente en el circuito al que afecta. Los resultados del acoplamiento eléctrico y magnético son **señales de cross-talk** (efecto no deseado producido por un canal de transmisión sobre otro canal de transmisión) en el circuito afectado. Existen varios parámetros que caracterizan la estabilidad del cable contra el cross-talk.

El **cross-talk de extremo cercano** (**NEXT**, por sus siglas en inglés) determina la estabilidad del cable en caso de que el cross-talk sea inducido como resultado de la influencia de la señal generada por el transmisor conectado a uno de los pares vecinos del lado del cable en el que



P_{sal} — Potencia de la señal a la salida del transmisor
P_{ind} — Potencia inducida de la señal en el extremo cercano al cable
$P_{ind\text{-}lejana}$ — Señal inducida en el extremo lejano del cable

FIGURA 8.10 Atenuación transitoria.

opere el receptor conectado al par afectado (figura 8.10). El parámetro NEXT expresado en decibeles es igual a 10 lg P_{sal}/P_{end}, donde P_{sal} es la potencia de la señal de salida y P_{ind} es la potencia de la señal inducida.

A medida que el valor NEXT es más pequeño (tomando en cuenta su signo), el cable será mejor. Por ejemplo, para un par trenzado de categoría 5, el valor NEXT debe ser menor que −27 dB a 100 MHz.

El **cross-talk de extremo lejano (FEXT,** por sus siglas en inglés) permite evaluar la estabilidad del cable contra el cross-talk cuando el transmisor y el receptor se encuentran conectados a diferentes lados del cable (y a pares distintos). Este parámetro de la línea suele ser mejor (más pequeño) que el NEXT, ya que la señal llega al extremo lejano del cable y es atenuada por el desvanecimiento de cada uno de los pares.

Como regla, los parámetros NEXT y FEXT se utilizan con un cable formado por varios pares trenzados, debido a que el cross-talk mutuo puede alcanzar valores impresionantes. Para un cable coaxial de un solo alambre (es decir, uno que esté formado por un solo hilo con protección), este parámetro no tiene sentido. Para el caso de un cable coaxial con dos hilos, este parámetro no se utiliza debido a la alta protección de cada hilo. Las fibras ópticas no generan ningún ruido entre sí digno de tomarse en cuenta.

Debido a que algunas tecnologías de red actuales implementan de manera simultánea la transmisión de datos por medio de varios pares trenzados, los parámetros de cross-talk se han presentado recientemente con el prefijo **PowerSUM** (PS), por ejemplo: **PS-NEXT** y **PS-FEXT**. Estos parámetros reflejan la estabilidad del cable contra la potencia total del cross-talk que afecta un solo par de cable y que se origina a partir de todos los pares restantes que conforman el cable (figura 8.11).

La **protección del cable** que representa la **relación atenuación/cross-talk (**ACR) constituye otra característica importante del cable. Dicha protección se define como la diferencia entre el nivel efectivo de la señal y el correspondiente del ruido. A medida que el valor ACR es mayor, será mayor la velocidad de datos potencial a la que este cable podrá transmitir datos de acuerdo con la fórmula de Shannon. La figura 8.12 muestra una característica típica que refleja la dependencia del ACR del cable de par trenzado sin protección con respecto a la frecuencia de la señal.

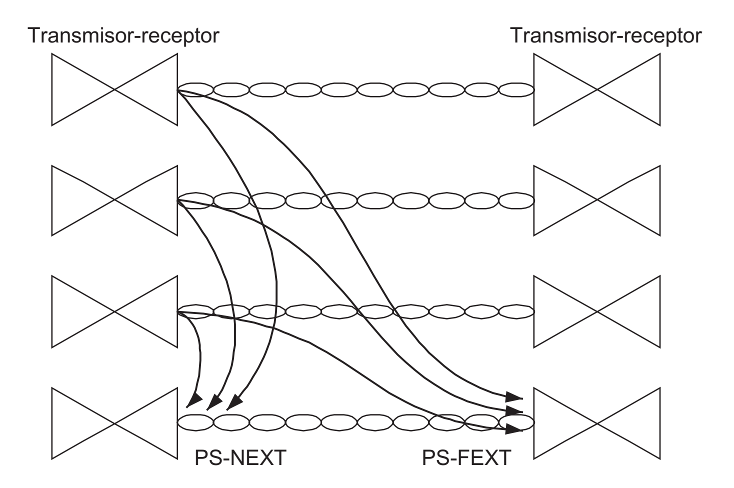


FIGURA 8.11 Atenuación transitoria total.

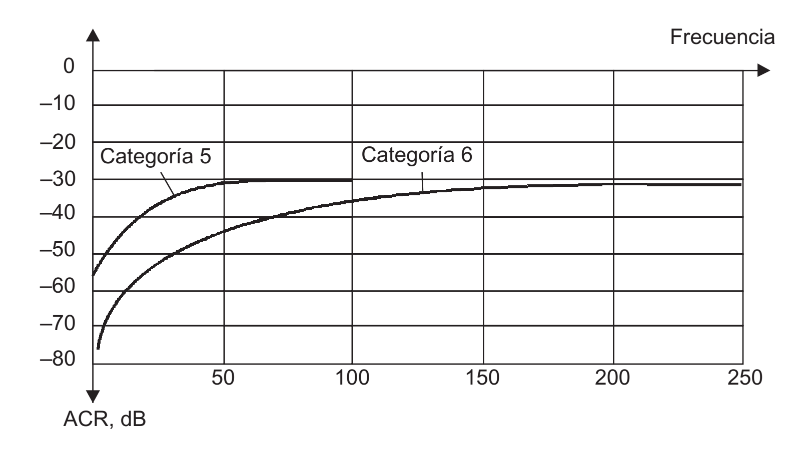


FIGURA 8.12 ACR de un par trenzado sin protección.

La **confiabilidad de la transmisión de datos** caracteriza la probabilidad de distorsión en cualquiera de los bits de los datos transmitidos. A veces este parámetro recibe el nombre de **tasa de errores** (**BER**). Como regla, el valor BER para los enlaces de comunicaciones sin equipo adicional para la corrección de errores (por ejemplo, códigos de autocorrección o protocolos que soporten la retransmisión de tramas distorsionadas) es de 10^{-4} a 10^{-6}. En las líneas de fibra óptica, éste sería de 10^{-9}. Un valor de la confiabilidad de la transmisión de datos de, digamos, 10^{-4} es una evidencia de que, en promedio, solamente 1 de 10 000 bits transmitidos está distorsionado.

8.3.4 Ancho de banda y capacidad

El **ancho de banda** es un rango de frecuencias continuo para el cual la atenuación de la línea no excede un valor límite predefinido. Esto significa que el ancho de banda determina el rango de frecuencias de una señal senoidal dentro del cual dicha señal se transmite a través de la línea sin distorsiones significativas.

A menudo, los límites de la frecuencia se toman como las frecuencias a las que la potencia de la señal de salida disminuye dos veces en comparación con la señal de entrada, misma que corresponde a una atenuación de –3 dB. Como se explicará más adelante, el ancho de banda ejerce una enorme influencia en la velocidad máxima alcanzable en los sistemas de transmisión de datos que utilizan enlaces de comunicaciones.

El ancho de banda depende del tipo de línea y de su longitud. La figura 8.13 muestra el ancho de banda de los tipos más populares de enlaces de comunicaciones, así como los rangos de frecuencia que se utilizan más ampliamente en las diferentes tecnologías.

La **capacidad del enlace** determina la velocidad máxima posible de transferencia de información que puede alcanzar una línea. Dicha característica depende de los parámetros del *medio de transmisión físico*. También está determinada por el *método de transmisión de datos*. En consecuencia, es imposible hablar acerca de capacidad de la línea antes de definir un protocolo de la capa física para ella.

Por ejemplo, debido a que el protocolo de la capa física que especifica la velocidad de transmisión de datos de los enlaces digitales está siempre definido, la eficacia de dichos enlaces siempre se conoce con antelación: 64 Kbps, 2 Mbps, y así sucesivamente.

Cuando es necesario determinar el protocolo existente que pueda ser usado en un enlace específico, otras características del enlace, como el ancho de banda, parámetros de cross-talk e inmunidad al ruido, adquieren gran importancia.

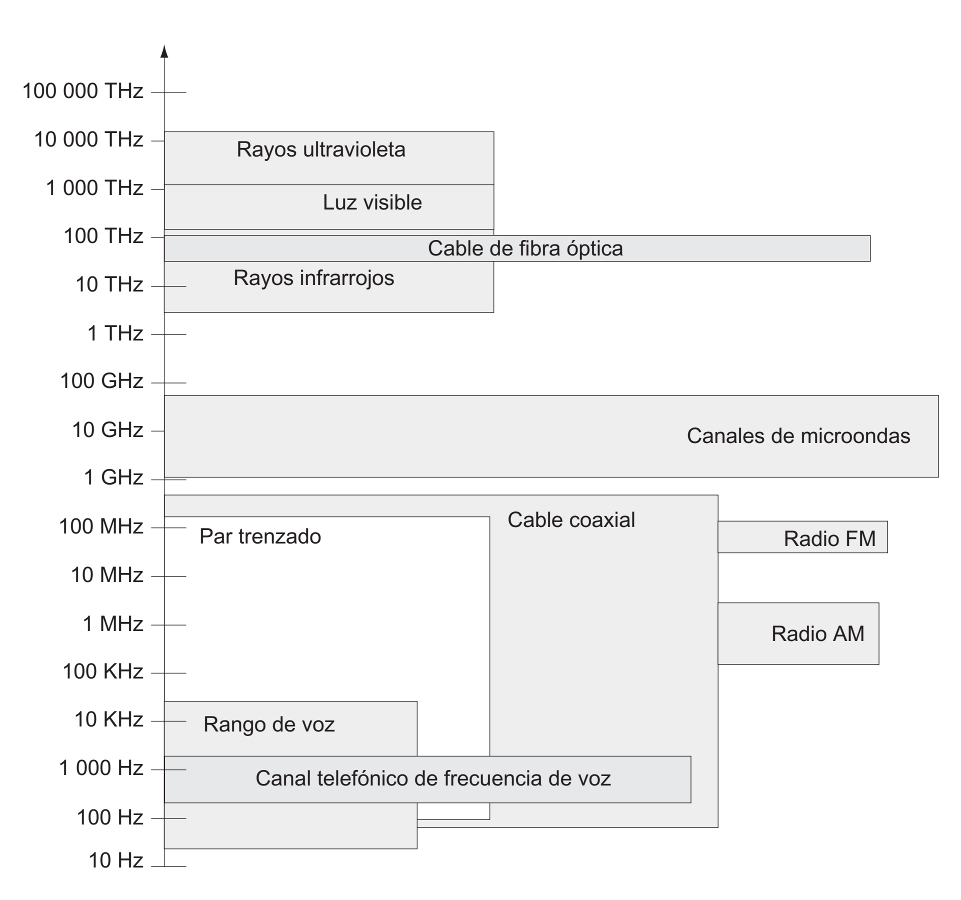


FIGURA 8.13 Ancho de banda de los tipos de enlaces de comunicaciones más utilizados y rangos de frecuencia más populares.

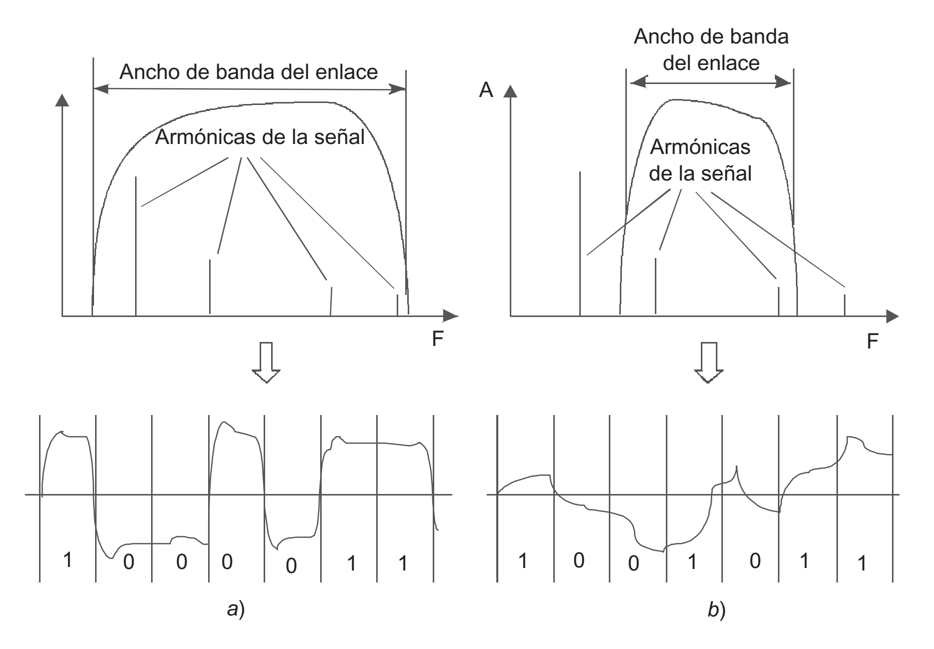


FIGURA 8.14 Correspondencia entre el ancho de banda del enlace y el espectro de la señal.

La capacidad, que es un parámetro similar a la velocidad de la información, se mide en bits por segundo, así como en unidades derivadas, tales como kilobits por segundo (Kbps).

NOTA *La capacidad y la velocidad de transferencia de información (uso) de los enlaces y del equipo de comunicaciones se miden tradicionalmente en bits por segundo en vez de bytes por segundo. Esto se debe a que los datos en las redes se transmiten de forma secuencial, bit por bit, en lugar de transmitirse en paralelo (en bytes) como sucede en los dispositivos internos de las computadoras. Entre las tecnologías de red, las unidades de medición tales como el kilobit, megabit y gigabit corresponden a potencias de 10 (lo cual significa que 1 Kb son 1 000 bits y 1 Mb es 1 000 000 bits) en lugar de potencias de 2 como en programación, donde 1 KB =* 2^{10} *= 1 024 y 1 MB =* 2^{20} *= 1 048 576.*

La capacidad del enlace depende no solamente de las características tales como la atenuación y el ancho de banda, sino también del espectro de señales que se transmiten. Si las armónicas significativas de la señal (es decir, las amplitudes que hacen las principales contribuciones a la señal resultante) se ubican dentro del ancho de banda del enlace, éste transmitirá dichas señales de alta calidad y los receptores podrán ser capaces de reconocer correctamente la información enviada por el transmisor a través del enlace (figura 8.14*a*). Si un número significativo de armónicas se halla fuera de los límites del ancho de banda de enlace, la señal será distorsionada de manera significativa y el receptor cometerá errores durante el reconocimiento de la información (figura 8.14*b*).

8.3.5 Bits y bauds

La selección del método para representar información discreta como las señales proporcionadas a un enlace de comunicaciones se conoce como *codificación física o de línea.* El espectro de la señal y, en consecuencia, el uso del enlace depende del método de codificación seleccionado.

Por lo tanto, para métodos de codificación diferentes, la capacidad del mismo enlace puede ser distinta. Por ejemplo, el par trenzado de categoría 3 puede transmitir datos con un ancho de banda de 10 Mbps cuando se utilice el método de codificación a nivel físico 10Base-T. Si se emplea el método de codificación estándar 100Base-T4, la capacidad del enlace será de 33 Mbps.

ATENCIÓN *De acuerdo con el postulado principal de la teoría de la información, cualquier cambio distinto e impredecible de la señal recibida lleva cierta información. De aquí que la recepción de la senoidal de amplitud, fase y frecuencia constante no lleva ninguna información, pues a pesar de que se presentan cambios en la señal, éstos son predecibles. De manera similar, los pulsos de reloj en la línea de reloj del bus de control, el cual es parte del bus del sistema de la computadora, no llevan información debido a que sus cambios son predecibles. Los pulsos en el bus de datos no pueden predecirse con antelación, característica que los hace informativos, porque dichos pulsos llevan información entre las unidades de cómputo o dispositivos.*

La mayoría de los métodos de codificación modifican un parámetro específico de la señal periódica —frecuencia senoidal, amplitud o fase, o el signo potencial de la secuencia de pulsos—. Un parámetro modificado de la señal periódica se conoce como **señal portadora** o **frecuencia de la portadora**, siempre y cuando la senoidal sea utilizada como dicha señal. El proceso que consiste en modificar los parámetros de la señal portadora de acuerdo con la información que necesita transmitirse se llama **modulación**.

Si la señal se modifica de tal manera que sea posible distinguir dos estados solamente, cada cambio en dicha señal corresponderá a 1 bit: la unidad más pequeña de información. Si la señal tiene más de dos estados diferentes, cualquiera de sus cambios llevará *varios bits de información.*

La transmisión de información discreta en las redes de telecomunicaciones es temporizada, lo cual significa que la señal cambia después de un intervalo de tiempo constante llamado señal de **reloj**. Esto significa que el receptor considera que al comienzo de cada intervalo llega nueva información a su entrada. Si se toma en cuenta lo anterior, el receptor obtiene nueva información proveniente del transmisor, ya sea que la señal repita el estado del reloj anterior o no, o bien tenga el estado diferente del anterior. Por ejemplo, si el reloj tiene una duración de 0.3 segundos y la señal tiene dos estados, donde el 1 está codificado con un potencial de 5 V, la presencia de la señal de 5 V en la entrada del receptor durante 3 segundos es equivalente a la entrega de información representada por el valor binario siguiente: 1111111111.

El número de cambios del parámetro de información de la señal portadora por segundo se mide en *bauds*. Un baud es igual a un cambio del parámetro de información por segundo. El tiempo entre dos cambios en la señal de información se conoce como reloj del transmisor.

IMPORTANTE *La velocidad de información generalmente no es igual a la velocidad en bauds. La primera puede ser mayor, menor o igual a la velocidad en bauds. Esta relación depende del método de codificación que se seleccione.*

Si la señal tiene más de dos estados distintos, la velocidad de información en bits por segundo será *mayor* que la velocidad en bauds. Suponga que hemos seleccionado la fase y amplitud de la senoide como parámetros de información y que tenemos cuatro estados discernibles de la fase —0, 90, 180 y 270 grados— y dos valores distintos de la amplitud de la señal. Esto significa que la señal de información puede tener hasta ocho estados diferentes. En consecuencia, cada cambio en esta señal lleva 3 bits de información. En este caso, un

módem que opera a una velocidad de 2 400 bauds (quiere decir que es capaz de cambiar la señal de información 2 400 veces por segundo) transmite información a una velocidad de 7 200 bps, ya que cada cambio de la señal transmite 3 bits de información.

Si la señal tiene solamente dos estados (lo cual significa que lleva 1 bit de información), la velocidad de información generalmente corresponde a la velocidad en bauds; sin embargo, la situación puede ser la opuesta: la velocidad de información puede ser menor que la velocidad en bauds. Esto sucede cuando, para garantizar el reconocimiento confiable de la información del usuario por el receptor, cada bit de la secuencia se codifica mediante varios cambios del parámetro de información de la señal portadora. Por ejemplo, cuando se representa el valor uno, mediante un pulso con polaridad positiva, y el valor cero, por un pulso con polaridad negativa, la señal física cambia su valor dos veces cuando transmite cada bit. Cuando se utiliza dicho método de codificación, la velocidad en bits es dos veces menor que la velocidad en bauds.

A medida que la frecuencia de la señal portadora es mayor, podrá ser más alta la frecuencia de modulación. En consecuencia, podrá obtenerse una utilización más alta del enlace de comunicaciones.

No obstante, el ancho espectral de la señal portadora aumenta a medida que crece su frecuencia. La línea transmite este espectro con distorsiones definidas por su ancho de banda. A medida que existe mayor disparidad entre el ancho de banda del enlace y el ancho del espectro de las señales de información transmitidas, éstas experimentarán mayor distorsión y la probabilidad de que aparezcan errores en el extremo receptor será más elevada. Por lo tanto, la velocidad de información posible será menor.

8.3.6 Dependencia entre el ancho de banda y la capacidad

La relación entre el ancho de banda del enlace y su capacidad, independientemente del método de codificación física seleccionado, fue establecida por *Claude Shannon:*

$$C = F \log_2 (1 + P_c/P_{\text{ruido}}) \tag{8.3}$$

Aquí, C es la capacidad del enlace en bits por segundo, F el tamaño del ancho de banda del enlace en Hertz, P_c la potencia de la señal y P_{ruido} la potencia del ruido.

A partir de esta fórmula, se puede deducir que no existe un límite teórico en la utilización de la línea con un ancho de banda constante; sin embargo, en la práctica existe dicho límite. Se podrá aumentar la capacidad del enlace si se incrementa la potencia del transmisor o si se reduce el ruido en la línea. Ambos componentes son difíciles de modificar. El aumento en la potencia del transmisor incrementa de manera significativa su tamaño y costo. La reducción del nivel de ruido requiere usar cables especiales con una protección de alta calidad, lo cual es muy costoso, así como la reducción del ruido en el transmisor y equipo de tránsito, lo que es difícil de lograr. Además, la influencia de las potencias de la señal efectiva y del ruido en la capacidad, está limitada por una dependencia logarítmica, la cual crece más despacio que la dependencia proporcional. Lo anterior resulta en un valor inicial típico de relación señal a un ruido de 100. La duplicación de la potencia del transmisor incrementa la capacidad de la línea solamente en 15 por ciento.

Existe otra relación deducida por *Harry Nyquist* y parecida a la fórmula de Shannon que determina la utilización máxima de un enlace de comunicaciones (por ejemplo, su capacidad). Sin embargo, ésta no toma en cuenta el ruido en la línea:

$$C = 2F \log_2 M \tag{8.4}$$

Aquí, M es el número de estados distintos del parámetro de información.

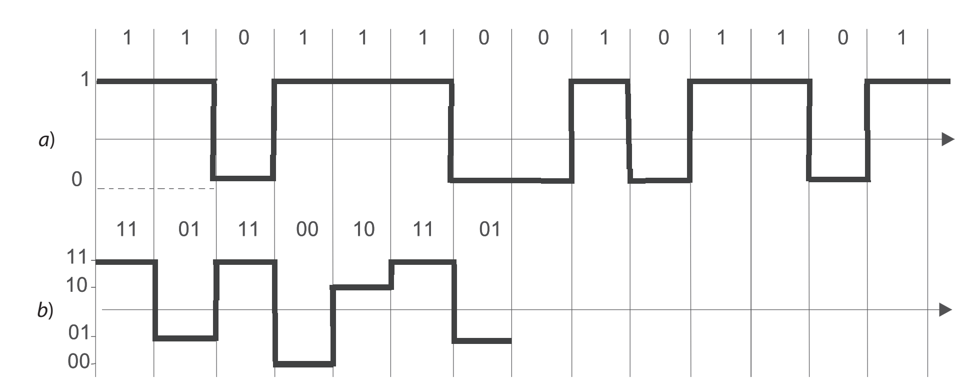


FIGURA 8.15 Aumento de la velocidad de transferencia de información mediante la adición de estados de la señal.

Si la señal tiene dos estados diferentes, la utilización es igual al doble del ancho de banda del enlace (figura 8.15*a*). Si el transmisor usa más de dos estados estables de la señal disponible para la codificación de datos, aumentará el empleo de la línea. Esto se debe a que el transmisor envía varios bits de datos por cada reloj —por ejemplo, 2 bits, siempre y cuando estén disponibles cuatro estados diferentes de la señal (figura 8.15*b*)—.

Aunque la fórmula de Nyquist no toma en cuenta de manera explícita el ruido, su influencia se refleja implícitamente en el número de opciones de los estados de la señal de información. Para incrementar la capacidad del enlace, tiene sentido aumentar el número de estados de la señal. Sin embargo, en la práctica, el ruido en la línea representa un obstáculo para usar este método. Por ejemplo, la capacidad de la línea (figura 8.15*b*) puede duplicarse una vez más, siempre que se utilicen 16 niveles de señal para la codificación de datos en lugar de 4; pero si la amplitud del ruido excede de vez en cuando la diferencia entre capas adyacentes, los receptores podrían no ser capaces de reconocer los datos transmitidos de manera confiable. Por lo tanto, el número de estados posibles de la señal está limitado por la relación entre la potencia de la señal efectiva y la potencia del ruido, y la fórmula de Nyquist determina la velocidad máxima de transmisión cuando el número de estados se ha seleccionado tomando en cuenta la posibilidad de que el receptor reconozca lo estable de la señal.

8.4 TIPOS DE CABLES

PALABRAS CLAVE: par trenzado con y sin protección, cable coaxial, cable de fibra óptica, categorías de cables, tipos de cables, cable coaxial “delgado”, cable coaxial “esbelto”, cable de televisión, fibra óptica multimodo (MMF), MMF con un cambio en el factor de refracción, fibra óptica monomodo (SMF), modo de rayo y sistema de cableado estructurado (SCS).

En la actualidad se utilizan tres clases de líneas de comunicación cableadas tanto en interiores como en exteriores:

- *Par trenzado.*
- *Cables coaxiales.*
- *Cables de fibra óptica.*

8.4.1 Par trenzado con protección y sin protección

Un par de alambres trenzados se conoce como **par trenzado.** Este tipo de medio de transmisión es muy conocido y constituye la base de la mayoría de los cables instalados tanto en interiores como en exteriores. Un cable puede contener varios pares trenzados. A veces, los cables externos cuentan con decenas de dichos pares.

El trenzado de los alambres reduce la influencia de ruidos externos y de cross-talk en las señales transmitidas a través del cable.

Las características principales de la construcción del cable se describen brevemente en la figura 8.16.

Los cables basados en un par trenzado son cables *simétricos*, los cuales están compuestos de dos alambres idénticos en construcción. Los cables simétricos pueden ser con protección, basados en STP, o sin protección, basados en UTP.

Es necesario distinguir al *aislamiento eléctrico* de los alambres conductores, que están presentes en cualquier cable, del *aislamiento electromagnético*. El aislamiento eléctrico consiste en capas aislantes de papel o polímeros, como el cloruro de polivinilo (PVC) o el poliestireno. Además del aislamiento eléctrico, los conductores se encuentran encerrados dentro de una protección electromagnética, que con mucha frecuencia consiste en una protección de cobre.

El cable de cobre para el cableado en interiores con base en pares trenzados sin protección está clasificado en varias **categorías** de acuerdo con los estándares internacionales (categoría 1 a categoría 7).

- Los cables clasificados como **categoría 1** se utilizan cuando los requerimientos para las velocidades de transmisión son mínimos. En general, éste es el cable que se usa en la transmisión de voz analógica y digital, la cual es apropiada también para la transmisión de datos a baja velocidad (hasta 20 Kbps). Hasta 1983, éste fue el tipo de cable principal empleado para telefonía.
- Los cables de **categoría 2** fueron utilizados por primera vez por IBM en la construcción de su sistema propietario de cableado. El requisito principal de los cables de esta categoría reside en su capacidad para transmitir señales con un espectro de hasta 1 MHz.

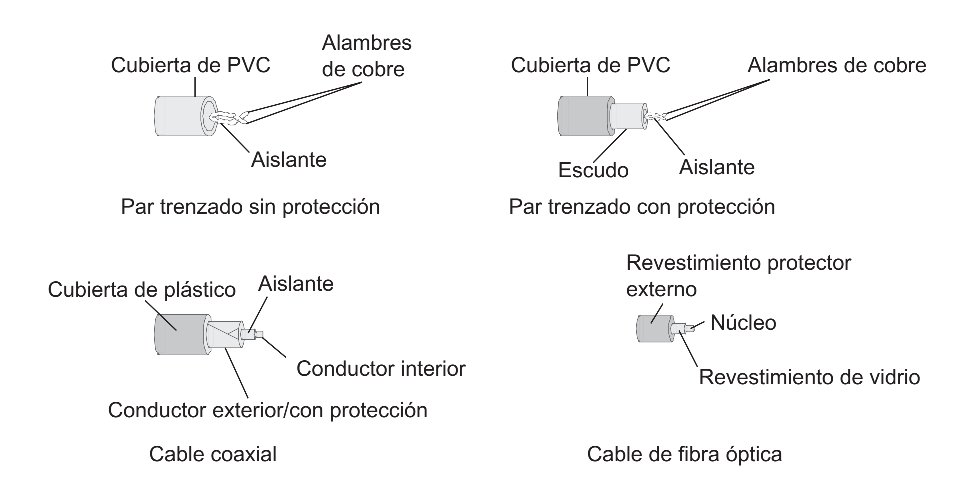


FIGURA 8.16 Diseño del cable.

- Los cables de **categoría 3** se estandarizaron en 1991 al diseñarse el *estándar de sistemas de cableado para las telecomunicaciones para edificios comerciales* (EIA-568), con base en el cual se diseñó el estándar actual EIA-568A. El estándar EIA-568 define las características eléctricas de los cables de categoría 3 dentro de un rango de frecuencia de hasta 16 MHz. Por lo tanto, los cables de esta categoría son capaces de soportar aplicaciones de red de alta velocidad.
- Los cables de **categoría 4** representan una versión mejorada de los cables de categoría 3. Los primeros deben soportar pruebas a frecuencias de transmisión de señales de 20 MHz y garantizar una inmunidad al ruido mejorada, así como bajas pérdidas de señal. En la práctica se utilizan muy rara vez.
- Los cables de **categoría 5** se diseñaron específicamente para soportar protocolos de alta velocidad. Por lo tanto, sus características están determinadas hasta 100 MHz. La mayoría de los estándares de alto desempeño están orientados hacia el uso del par trenzado categoría 5. Este cable se utiliza con protocolos de alta velocidad a velocidades de transmisión de datos de 100 Mbps, como FDDI, Fast Ethernet y protocolos más rápidos —ATM a 155 Mbps y Gigabit Ethernet a 1 000 Mbps—. El cable de categoría 5 ha reemplazado al cable de categoría 3 y en la actualidad este tipo de cable (junto con el de fibra óptica) se utiliza para instalar nuevos sistemas de cableado en grandes edificios.
- La industria comenzó a fabricar cables de **categorías 6** y **7** hasta fechas muy recientes. En el cable de categoría 6, las características están definidas hasta una frecuencia de 250 MHz. Para los cables de categoría 7, dicha frecuencia es de hasta 600 MHz. Los cables de esta última categoría deben contar con protección, la cual deberá aplicarse tanto a cada par como al cable entero. Un cable de categoría 6 puede tener protección o no. Estos cables se diseñaron principalmente para soportar protocolos de alta velocidad en secciones más largas de cable que las que soporta el cable UTP de categoría 5.

Independientemente de su categoría, todos los cables UTP están fabricados como cables de 4 pares. Cada par tiene un color y una disposición de los alambres específicos. En general, se utilizan dos pares para la transmisión de datos y dos para la transmisión de voz.

El par trenzado con protección evita que la señal transmitida sea afectada por fuentes externas. Además de esto, se caracteriza por una emisión más baja de ondas electromagnéticas, con lo cual se protege a los usuarios de la red de la dañina radiación electromagnética. Sin embargo, la presencia de la protección aterrizada eleva el precio del cable y dificulta los procesos de instalación, ya que se requiere un sistema de tierra de alta calidad.

El estándar propietario de IBM es el estándar principal que determina el parámetro del par trenzado con protección para su uso dentro de edificios. De acuerdo con este estándar, los cables se clasifican por tipos y no por categorías: tipo 1, tipo 2,…, tipo 9.

Un cable *tipo 1* de acuerdo con el estándar de IBM incluye dos pares de alambres trenzados protegidos mediante un armado de cable conductor, el cual está aterrizado. Los parámetros eléctricos del cable tipo 1 corresponden de manera aproximada a los de los cables UTP de categoría 5. Sin embargo, la impedancia del cable tipo 1, la cual es de 150 ohms, es significativamente mayor que la del cable UTP de categoría 5 (100 ohms). Por lo tanto, una mejora en el armado del cable mediante el simple reemplazo del UTP sin protección con el STP tipo 1 es imposible. Los transmisores diseñados para trabajar con el cable que tiene una impedancia de 100 ohms no trabajarán de manera satisfactoria con un cable que tenga una impedancia de 150 ohms.

8.4.2 Cable coaxial

El **cable coaxial** consiste en pares de conductores *asimétricos*. Cada par está formado por un alambre de cobre interno y un alambre coaxial externo, el cual puede ser un tubo de cobre hueco o un armado separado de sus alambres internos mediante un aislamiento dieléctrico. El alambre externo desempeña un doble papel. Primero, se utiliza para transmitir señales con información; segundo, es un escudo que protege al alambre interior de los campos electromagnéticos externos. Existen varios tipos de cable coaxial, los cuales difieren en sus características y áreas de aplicación, para LAN, WAN, redes de telecomunicaciones, televisión por cable, etcétera.

Los estándares actuales no contemplan al cable coaxial como una buena opción para su uso en sistemas de cableado estructurado para edificios. A continuación se proporcionan los tipos y características principales de estos cables de acuerdo con la clasificación de Estados Unidos:

- Los **cables coaxiales "gruesos"** se diseñaron para las redes Ethernet 10Base-5. Tienen una impedancia igual a 50 ohms y un diámetro exterior de 0.5 pulgadas (alrededor de 12 mm). Estos cables tienen un conductor interno delgado (2.17 mm de diámetro), lo cual garantiza buenas características mecánicas y eléctricas (atenuación a 10 MHz no mayor que 18 dB/km). Sin embargo, estos cables no son flexibles y, por lo tanto, son difíciles de instalar.
- Los **cables coaxiales "delgados"** para redes Ethernet 10Base-2. Este cable tiene una impedancia de 50 ohms, pero sus características mecánicas y eléctricas son significativamente inferiores a las del cable coaxial grueso. Los conductores internos delgados tienen diámetros de 0.89 mm y no son rígidos, sino flexibles y, por lo tanto, apropiados para instalar el cable. La atenuación de este tipo de cable es mayor que la del cable grueso, lo cual da como resultado la reducción de la longitud del cable con el fin de obtener la misma atenuación dentro de un segmento determinado.
- El **cable de televisión** tiene una impedancia igual a 75 ohms. Se utiliza ampliamente en sistemas de televisión por cable. Existen estándares de LAN que usan este cable para la transmisión de datos.

8.4.3 Cable de fibra óptica

El cable de **fibra óptica** consiste en fibras (guías de onda ópticas) de vidrio flexible delgadas (de 5 a 60 μm) a lo largo de las cuales se propagan señales luminosas. Este tipo de cable tiene la mejor calidad, ya que garantiza la transmisión de datos a una velocidad muy elevada (a 10 Gbps o mayor). Además, garantiza una mejor protección de los datos contra el ruido externo que cualquier otro medio de transmisión. Debido a las características especiales de la propagación de la luz, dichas señales pueden protegerse con mucha facilidad.

Cada guía de onda de luz consiste en una guía de onda central (núcleo) —fibra óptica— y una cubierta de vidrio con un factor de refracción menor que el del núcleo. Las ondas luminosas se propagan a través del núcleo sin abandonarlo, ya que éstas se reflejan en la capa que forma la cubierta. Según la distribución del factor de refracción y del diámetro del núcleo, los cables de fibra óptica se clasifican en las categorías siguientes:

- Fibras multimodo (MMF) con cambio abrupto del factor de refracción (figura 8.17*a*)
- MMF con cambio gradual del factor de refracción (figura 8.17*b*)
- Fibra monomodo (SMF) (figura 8.17*c*)

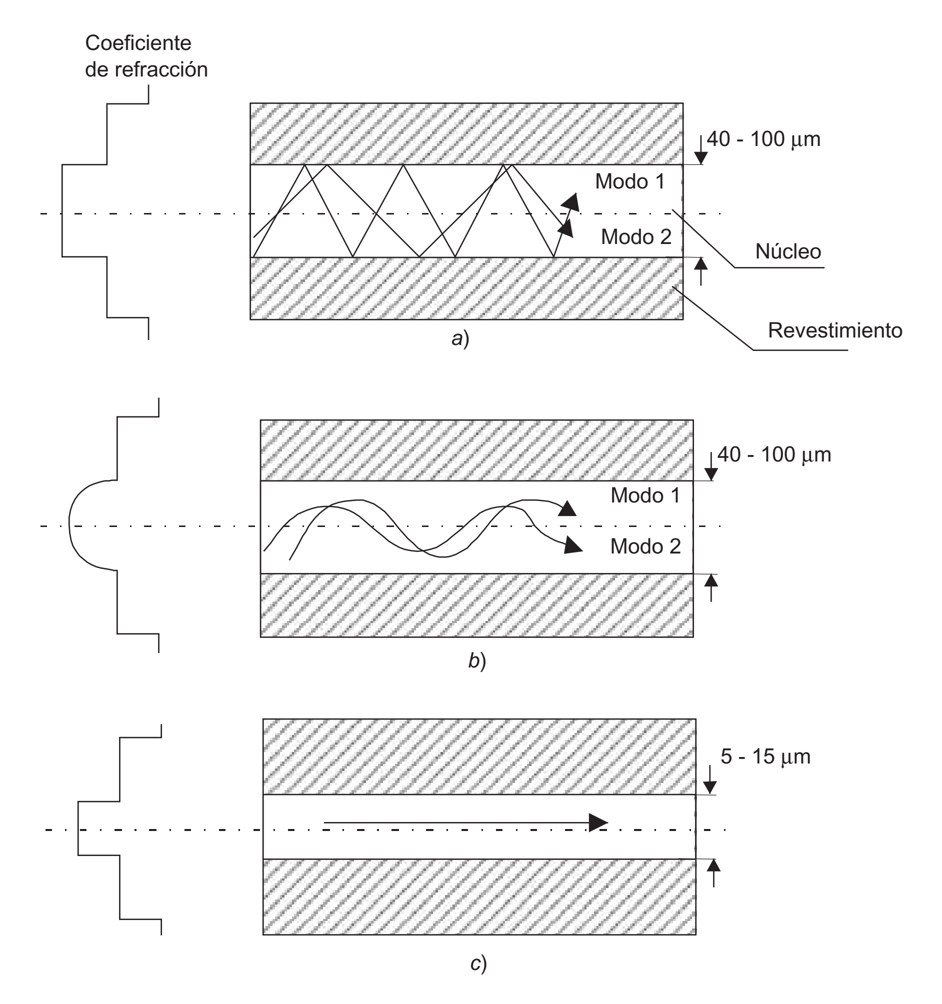


FIGURA 8.17 Tipos de cables de fibra óptica.

El concepto de modo describe la forma de propagación de los rayos de luz dentro del núcleo interior del cable. En las fibras **SMF**, el núcleo central tiene un diámetro muy pequeño en comparación con la longitud de onda de la luz, de 5 a 10 μm. En estas condiciones, prácticamente todas las ondas de luz se propagan a través del eje óptico de la guía de ondas sin reflejarse en la cubierta exterior. La fabricación de cable de fibras *SMF* de alta calidad es un proceso complejo desde el punto de vista tecnológico. En consecuencia, el cable óptico *SMF* es costoso; además, es difícil de enviar un rayo de luz a través de una fibra con un diámetro tan pequeño sin perder una parte significativa de su energía.

En los cables **MMF** se utilizan núcleos interiores más anchos, lo cual facilita significativamente su manufactura. En dichos cables, el núcleo conduce varios rayos de luz de manera simultánea. Dichos rayos se reflejan en la cubierta exterior con diferentes ángulos. El ángulo de reflexión del rayo de luz se llama **modo de rayo.** En los cables multimodo con cambio del factor de refracción gradual, la naturaleza de cada modo de propagación es muy compleja. La interferencia de los rayos de los diferentes modos degrada la calidad de la señal que se transmite, lo cual resulta en distorsiones de los pulsos transmitidos. Los cables *MMF* son más fáciles de fabricar; por lo tanto, son considerablemente más baratos que los cables monomodo. Al mismo tiempo, sus características son bastante más pobres que las de los cables monomodo.

Como resultado, los cables multimodo se utilizan principalmente para transmitir datos a distancias más pequeñas (de 300 a 2 000 metros) a velocidades que no excedan 1 Gbps y los cables monomodo están diseñados para la transmisión de datos a las velocidades más elevadas posibles: decenas de gigabits por segundo (cuando se utiliza la tecnología DWDM, ésta puede ser aún de varios terabits por segundo), en distancias que van desde varios kilómetros (LAN y MAN) hasta decenas o aun cientos de kilómetros (comunicaciones a largas distancias).

Como fuentes luminosas, los cables de fibra óptica usan:

- Diodos emisores de luz (LED).
- Diodos láser.

En los cables monomodo, solamente se utilizan diodos láser; al tener diámetros tan pequeños la fibra óptica, el rayo de luz producido por el LED no puede acoplarse a la guía de ondas sin tener pérdidas significativas debidas a su ancho patrón de radiación direccional. El diodo láser, en contraste con el LED, tiene un diagrama direccional más angosto. Por esta razón, los LED se utilizan solamente para cables MMF.

El costo de los cables de fibra óptica no excede significativamente el de los cables que se basan en par trenzado. Sin embargo, el trabajo involucrado en la instalación de los cables de fibra óptica es difícil y costoso debido a la gran cantidad de trabajo que implican las operaciones de instalación y el elevado costo de los equipos para instalar la fibra óptica.

8.4.4 Sistema de cableado estructurado en edificios

El **sistema de cableado estructurado** (**SCS**) de un edificio es un conjunto de elementos de conmutación (cables, conectores, enchufes, tableros de conmutación y clósets), así como los métodos para su uso compartido, los cuales permiten crear estructuras de comunicaciones fáciles de expandir en las redes de computadoras. El edificio es una estructura regular por sí misma. Comprende diferentes pisos, cada uno de los cuales contiene un número específico de oficinas conectadas mediante pasillos. La estructura del edificio define la estructura del sistema de cableado.

El sistema de cableado estructurado de un edificio es una especie de bloques que el diseñador de la red utiliza para construir la configuración requerida a partir de cables estándar conectados con conectores estándar y conmutados con tableros de conmutación también estándares. Cuando es necesario, la configuración de las conexiones puede modificarse con gran facilidad. Por ejemplo, se puede agregar una computadora, un segmento o un switch, quitar equipo innecesario y modificar las conexiones entre las computadoras y los concentradores o hubs.

En la actualidad, los sistemas de cableado que se emplean en edificios comerciales están bien definidos. Un método jerárquico del proceso de creación de dichos sistemas de cableado se llama *estructurado*. Gracias al SCS instalado en los edificios comerciales, pueden operar varias LAN pertenecientes a distintas organizaciones o varios departamentos de una sola organización. El SCS está planeado y construido de manera jerárquica con base en una troncal principal y múltiples ramificaciones (figura 8.18).

La estructura jerárquica típica del SCS (figura 8.19) incluye:

- Los **subsistemas horizontales**, que corresponden a los pisos del edificio: éstos conectan clósets de conmutación del piso con los enchufes de los usuarios finales.

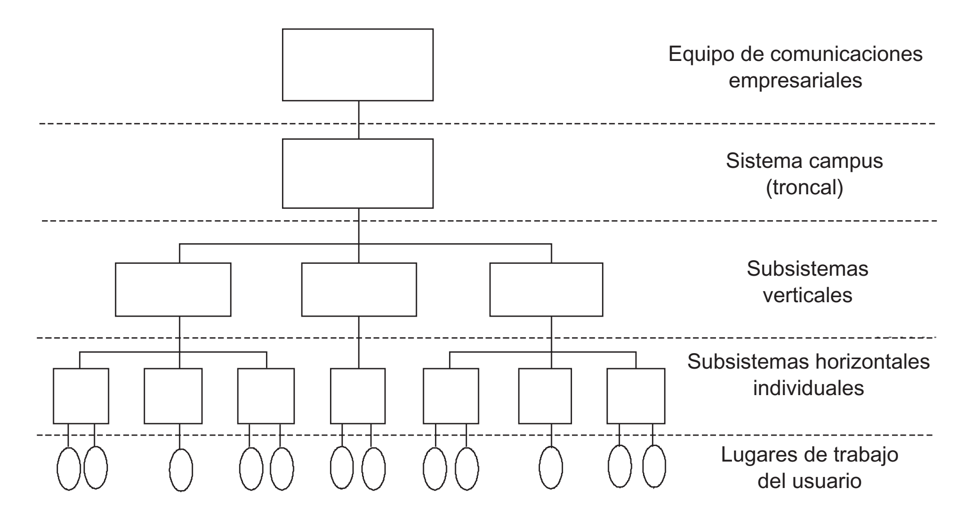


FIGURA 8.18 Jerarquía de los subsistemas de un sistema de cableado estructurado.

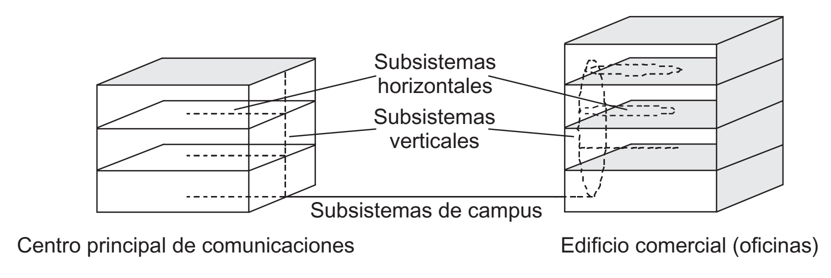


FIGURA 8.19 Estructura de los subsistemas de cableado.

- Los **subsistemas verticales**, que conectan los clósets de conmutación de cada piso con el cuarto donde se encuentra el equipo central de todo el edificio.
- El **subsistema de campus**, que conecta varios edificios al cuarto del equipo central de todo el campus. Esta parte del sistema de cableado generalmente se llama *troncal*.

Cuando se usa un sistema de cableado estructurado, los cables instalados en forma aleatoria proporcionan un gran número de ventajas a la empresa. *Si la* estructura SCS ha sido planeada cuidadosamente, podrá proporcionar un *medio de transmisión universal* para enviar datos de computadora en LAN, organizar la red telefónica local, transmitir información de video y aun enviar señales provenientes de sensores de sistemas contra fuego y de seguridad. Esto permite automatizar una gran cantidad de procesos de control, supervisión y administración de varios servicios empresariales, incluidos sistemas domésticos de seguridad y sistemas de seguridad personal.

Además, el uso de un SCS *permite que el proceso de adición de nuevos usuarios o que el cambio de sus espacios de trabajo sea más eficaz y económico.* Se sabe muy bien que el costo de un sistema de cableado está definido principalmente por el costo de su instalación más que por el costo del cable. En consecuencia, resulta mucho más eficaz instalar el cable previamente, aunque pueda haber redundancias con objeto de asegurar un buen desempeño. Esto es preferible a tener que instalar el cable varias veces simplemente extendiendo su longitud.

RESUMEN

- En función del tipo de equipo intermedio, todos los enlaces de comunicaciones se dividen en analógicos y digitales. En los enlaces analógicos (o canales analógicos), el equipo intermedio está diseñado para amplificar señales analógicas. Dichos enlaces utilizan el multiplexaje por división de frecuencia (FDM) o el multiplexaje por división de longitud de onda (WDM).
- En los enlaces digitales, las señales que se transmiten tienen un número finito de estados. Los canales digitales utilizan equipo intermedio especial. Así, los regeneradores mejoran la forma de los pulsos y garantizan su resincronización (es decir, restablecen los intervalos entre pulsos). El equipo de multiplexaje y conmutación intermedio de las redes de transmisión opera de acuerdo con el principio del multiplexaje por división de tiempo (TDM), en el cual a cada enlace a menor velocidad se le asigna una ranura de tiempo específica del canal de alta velocidad.
- El ancho de banda describe los rangos de frecuencia transmitidos por el enlace de comunicaciones con una atenuación aceptable.
- La capacidad del enlace depende de parámetros internos, en particular de su ancho de banda, de parámetros externos (como el nivel de ruido y el grado de supresión del ruido) y del método adoptado para codificar los datos digitales.
- La fórmula de Shannon define la capacidad del enlace de comunicaciones a valores constantes del ancho de banda del enlace y la relación entre la potencia de la señal y la potencia del ruido.
- La fórmula de Nyquist expresa la capacidad del enlace a través de su ancho de banda y del número de estados de la señal de información.
- Los cables de par trenzado pueden ser sin protección (UTP) o con ella (STP). Los cables UTP son más fáciles de fabricar e instalar, pero los cables STP aseguran un mejor nivel de protección.
- Los cables de fibra óptica poseen excelentes características electromagnéticas y mecánicas. Sin embargo, su principal desventaja consiste en su complicada y costosa instalación.
- Un sistema de cableado estructurado es un conjunto de elementos de comunicaciones —cables, conectores, ranuras, tableros y clósets de conmutación— que satisfacen estándares y permiten la creación de estructuras de comunicaciones fáciles de expandir.

PREGUNTAS DE REPASO

1. ¿Cuál es la diferencia entre un enlace de transmisión y un circuito?
2. ¿Pueden los circuitos incluir enlaces?, ¿pueden los enlaces incluir circuitos?
3. ¿Puede un canal digital transmitir datos analógicos?
4. ¿Cuáles son las funciones del DTE y del DCE?, ¿a qué tipo de dispositivos pertenecen los adaptadores de red?
5. ¿A qué tipo de características de enlaces de comunicaciones pertenecen los conceptos siguientes: nivel de ruido, ancho de banda y capacitancia lineal?
6. ¿Qué medidas se pueden tomar para incrementar la velocidad de transmisión de información de un enlace?
7. ¿Por qué no es siempre posible incrementar la capacidad del canal aumentando el número de estados de la señal de información?

8. ¿Qué mecanismo ayuda a eliminar el ruido en los cables UTP?
9. ¿Qué cable garantiza una mejor calidad en la transmisión de señales: el que tiene un valor más elevado del parámetro NEXT o el que tiene un menor valor de dicho parámetro?
10. ¿Cuál es el ancho espectral de un pulso ideal?
11. Liste los tipos de cable de fibra óptica.
12. ¿Qué pasaría si un cable UTP fuese reemplazado por un STP?
13. Haga una lista de las principales ventajas del sistema de cableado estructurado.
14. ¿Qué tipos de cables se utilizan para el subsistema horizontal del SCS?
15. ¿Cuáles son los problemas relacionados con el uso de cables de fibra óptica en los subsistemas horizontales?

PROBLEMAS

1. Se proporcionan los valores siguientes:
   - Potencia mínima de transmisor P_{sal} (dBm).
   - Atenuación del cable A (dB/km).
   - Umbral de sensibilidad del receptor P_{ent} (dBm).

   Encuentre la máxima longitud posible del enlace de comunicaciones a la que las señales se transmitirán de manera apropiada.
2. ¿Cuál será el límite teórico de la velocidad de transmisión (bps) utilizando el canal con un ancho de banda igual a 20 kHz si la potencia del transmisor es de 0.01 mW y el nivel de ruido del canal es de 0.0001 mW?
3. Determine la capacidad del enlace de comunicaciones dúplex en cada dirección siempre y cuando su ancho de banda sea de 600 kHz y el método de codificación utilice 10 estados de señal de información.
4. Calcule el retardo de propagación de la señal y el retardo de la transmisión de datos para enviar un paquete de 128 bytes (la velocidad de propagación de la señal se considera la misma que la de la luz en el vacío, es decir, 300 000 km/seg):
   - Utilizando un cable de par trenzado de 100 m a una velocidad de transmisión igual a 100 Mbps.
   - Usando un cable coaxial de 2 km a una velocidad de transmisión igual a 10 Mbps.
   - Utilizando un canal satelital de 72 000 km de longitud a una velocidad de transmisión de 128 Kbps.
5. Calcule la velocidad del canal, dado que la frecuencia de transmisión del reloj es de 125 MHz y la señal tiene cinco estados.
6. Los transmisores y receptores del adaptador de red están conectados a pares adyacentes de cable UTP. ¿Cuál es la potencia del ruido inducido a la entrada del receptor, siempre y cuando el transmisor tenga una potencia de 30 dBm y el parámetro NEXT del cable sea de 20 dB?
7. Siempre y cuando un módem transmita datos en modo dúplex a una velocidad de 33.6 Kbps, calcule cuántos estados tendrá la señal si el ancho de banda del canal es de 3.43 kHz.

9

CODIFICACIÓN Y MULTIPLEXAJE DE DATOS

DESCRIPCIÓN DEL CAPÍTULO

9.1 INTRODUCCIÓN

El medio de transmisión guiado que se estudió en el capítulo 8 proporciona solamente las posibilidades potenciales de transmitir información discreta. Para permitir que el transmisor y el receptor conectados con un medio de transmisión específico intercambien información, es necesario que estén de acuerdo en las señales que corresponderán a unos y a ceros binarios cuando se transmita información discreta. En el medio de transmisión se utilizan dos tipos de señales para representar información discreta: pulsos rectangulares y ondas senoidales. En el primer caso, el método para representar información discreta se conoce como codificación, mientras que en el segundo caso el método se llama modulación.

Existen muchos métodos de codificación, los cuales difieren en cuanto al ancho del espectro de la señal a la misma velocidad de transmisión de la información. Para transmitir información con un mínimo de errores, el ancho de banda del enlace debe ser más amplio que el espectro de la señal. Si no es así, las señales seleccionadas para representar ceros y unos serán distorsionadas de una manera significativa y el receptor no podrá reconocer correctamente la información transmitida. Por lo tanto, el espectro de la señal es uno de los criterios principales para evaluar la eficiencia del método de codificación seleccionado; además, el método de codificación debe ayudar al receptor a sincronizarse con el transmisor, a la vez que debe garantizar una relación señal-a-ruido aceptable. Dichos requerimientos son contradictorios; en consecuencia, cada método de codificación que se utilice representa un compromiso entre los requerimientos principales.

La presencia de errores en los enlaces de comunicaciones no puede eliminarse por completo, aun si el código seleccionado proporciona un buen nivel de sincronización y altos valores de la relación señal-a- ruido. Por lo tanto, cuando se transmite información discreta, se utilizan códigos especiales. Dichos códigos son capaces de detectar errores de bits y, algunos de ellos, de corregirlos.

En este capítulo se describirán al final los métodos de multiplexaje, los cuales proporcionan la posibilidad de contar con varios canales dentro de un solo enlace de comunicaciones.

9.2 MODULACIÓN

PALABRAS CLAVE: modulación, modulación de amplitud, modulación en frecuencia, modulación en fase, señales analógicas, señales discretas, manipulación por corrimiento de amplitud (ASK), manipulación por corrimiento de frecuencia (FSK), manipulación por corrimiento de fase (PSK), frecuencia de la portadora, modulador, demodulador, módem, código potencial, FSK binario (BFSK), FSK de cuatro niveles, FSK multinivel (MFSK), PSK binario (BPSK), PSK en cuadratura (QPSK), modulación de amplitud en cuadratura (QAM), códigos trellis, fórmula de Fourier y frecuencia fundamental.

9.2.1 Modulación cuando se transmiten señales analógicas

Históricamente, la modulación se usó en un principio para transmitir información **analógica** más que **discreta**.

La necesidad de modular información analógica surgió cuando fue necesario transmitir señales analógicas de baja frecuencia a través de canales que se ubicaban en el rango de alta frecuencia del espectro. Algunos ejemplos de dicha situación son la transmisión de voz por radio o televisión. La voz humana tiene un espectro con un ancho de aproximadamente

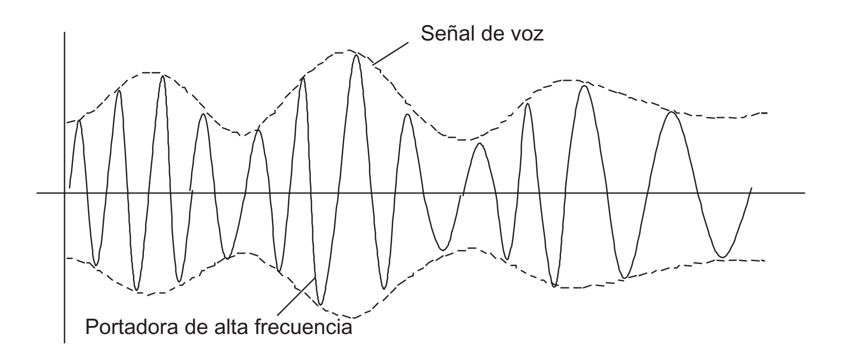


FIGURA 9.1 Modulación de la señal de voz.

10 KHz y en el rango del radio se usan frecuencias considerablemente mayores: de 30 kHz a 300 kHz. La televisión utiliza frecuencias aún más grandes. Como es obvio, la transmisión directa de voz a través de dicho medio de transmisión es imposible.

Por lo tanto, para resolver este problema, se decidió cambiar (modular) la amplitud de la señal de alta frecuencia de acuerdo con los cambios de la señal de baja frecuencia (figura 9.1). En este caso, el espectro de la señal resultante cabe perfectamente dentro del rango de altas frecuencias requerido. Este tipo de modulación se conoce con el nombre de **modulación de amplitud** (AM), ya que la amplitud de la señal de alta frecuencia es el parámetro que conlleva la información.

Además de la amplitud de la portadora, la frecuencia también puede emplearse como parámetro de la información. En dichos casos se trataría de la **modulación de frecuencia** (FM).[1]

La componente de alta frecuencia de la señal también se conoce con el nombre de *frecuencia de la portadora,* ya que esta señal desempeña el papel de portadora en relación con la señal de información de baja frecuencia.

9.2.2 Modulación cuando se transmiten señales discretas

Cuando se transmite información discreta mediante el uso de la modulación, los unos y los ceros se codifican cambiando la amplitud, frecuencia o fase de la señal portadora senoidal. En los casos en que las señales moduladas transmiten información discreta, se utiliza la terminología siguiente:

- Manipulación por corrimiento de amplitud (ASK).
- Manipulación por corrimiento de frecuencia (FSK).
- Manipulación por corrimiento de fase (PSK).

Quizás el ejemplo más conocido del uso de la modulación cuando se trasmite información discreta es la transmisión de datos de una computadora a través de líneas telefónicas. La característica típica de amplitud-frecuencia de una línea de abonado estándar, también llamada *canal de tonos,* se presenta en la figura 9.2. Este circuito pasa a través de los switches de tránsito de una red telefónica y conecta los aparatos telefónicos de los abonados. El canal

[1] Observe que cuando se modula información analógica, la fase no se utiliza como un parámetro de información.

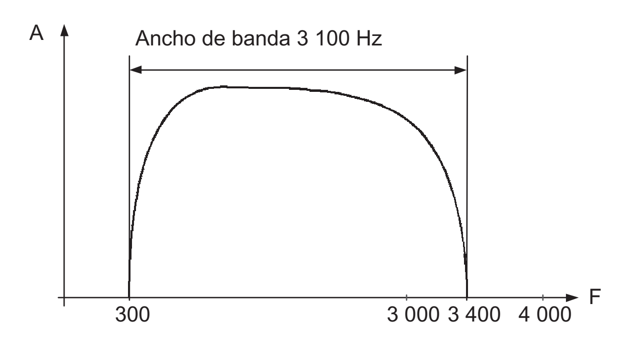


FIGURA 9.2 Características de amplitud-frecuencia del canal de tonos de frecuencia.

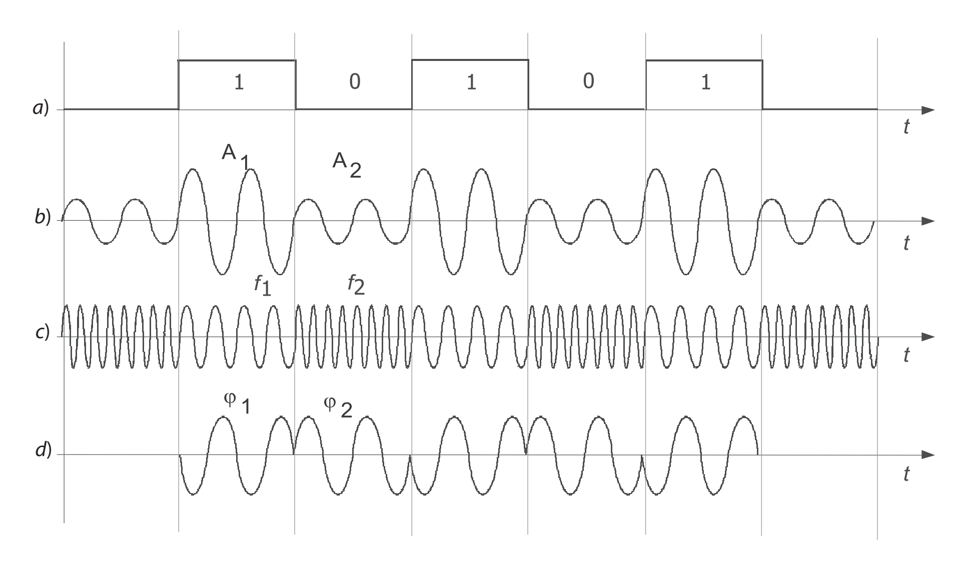


FIGURA 9.3 Diferentes tipos de modulación.

de tonos transfiere las frecuencias en el rango de 300 a 3 400 Hz; por lo tanto, su ancho de banda es igual a 3 100 Hz. Ese ancho de banda angosto es suficiente para transmitir voz de alta calidad; sin embargo, no es lo suficientemente ancha para transmitir datos de computadora en la forma de pulsos rectangulares. La solución a este problema reside en el uso de la manipulación por corrimiento de amplitud. El dispositivo que modula a la portadora senoidal del lado de transmisión y la demodula en el extremo receptor se conoce con el nombre de **módem** (**mod**ulador-**dem**odulador).

Los métodos principales de modulación que se utilizan para transmitir información discreta se muestran en la figura 9.3. El diagrama (figura 9.3*a*) revela la secuencia de bits de la fuente de información representada por voltajes con nivel alto para los unos lógicos, y voltajes con nivel cero para los ceros[2] lógicos. Dicho método de codificación se conoce como *código de potenciales* y se usa con frecuencia cuando se transmiten datos entre las diferentes unidades de una computadora.

Cuando se utiliza ASK (figura 9.3*b*), se seleccionan diferentes niveles de amplitud de la portadora para expresar los unos y ceros lógicos. Este método se emplea muy rara vez

[2] En general, los códigos potenciales utilizan dos valores para los ceros y unos lógicos: positivo para el uno y negativo para el cero.

debido a su pobre inmunidad al ruido; sin embargo, se utiliza con mucha frecuencia en la modulación PSK.

Cuando se usa FSK (figura 9.3*c*), los valores 0 y 1 de la fuente de datos se transmiten mediante señales senoidales a distintas frecuencias: f_0 y f_1. Este método de modulación no requiere implementar complejos circuitos en los módems y, como regla general, se utiliza en módems de baja velocidad que trabajan a velocidades de 300 y 1 200 bps. Cuando se usan sólo dos frecuencias, se transmite 1 bit de información por señal de reloj, por lo cual este método se llama *FSK binario (BFSK).* También es posible utilizar cuatro frecuencias para codificar 2 bits de información por señal de reloj. Este método se conoce con el nombre de *FSK de cuatro niveles.* También se usa otro término, llamado *FSK multinivel (MFSK).*

Cuando se utiliza PSK (figura 9.3*d*), las señales de la misma frecuencia pero de diferente fase (por ejemplo, 0° y 180° o 0°, 90°, 180° y 270°) corresponden a los valores 0 y 1. En el primer caso, dicha modulación se llama *PSK binario (BPSK);* la segunda variante se conoce como *PSK en cuadratura (QPSK).*

9.2.3 Métodos combinados de modulación

Con la finalidad de incrementar la velocidad de transferencia de datos, se utilizan métodos combinados de modulación. Los más comunes son los métodos de **modulación de amplitud en cuadratura** (QAM), *los cuales se basan en la combinación de la modulación de fase y la de amplitud.*

La figura 9.4 muestra la variante de modulación 16-QAM, en la que se usan ocho valores diferentes de fase y cuatro valores de amplitud. Sin embargo, solamente se utilizan 16 de 32 combinaciones de señales, pues los valores permitidos de amplitud difieren de las fases

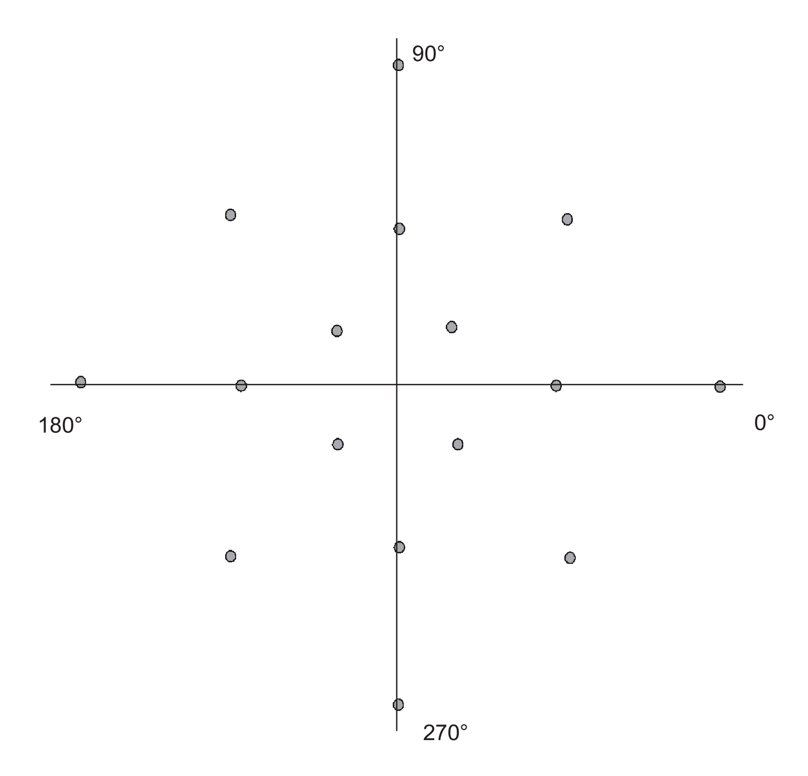


FIGURA 9.4 Modulación de amplitud en cuadratura con 16 estados de la señal.

vecinas. Esto mejora la inmunidad al ruido del código, pero la velocidad de transferencia de información disminuye dos veces. Otra solución para mejorar la confiabilidad del código a costa de la introducción de redundancia son los códigos trellis, los cuales *agregan un quinto bit a cada 4 bits de información. Este bit adicional le permite determinar con un alto grado de probabilidad el grupo correcto de 4 bits de información, aun cuando haya errores.*

El espectro de la señal modulada resultante depende del tipo y velocidad de la modulación (es decir, de la velocidad de transmisión deseable de la fuente de información).

Primero, considere el espectro de la señal cuando se utiliza la codificación potencial. Suponga que el valor lógico uno se codifica mediante un voltaje positivo y el cero mediante un voltaje negativo con el mismo valor. Para efectos de simplicidad, suponga que la información que se transmite consiste en una secuencia infinita de unos y ceros alternados, como se muestra en la figura 9.3*a*.

El espectro se puede deducir directamente a partir de la **fórmula de Fourier**[3] para funciones periódicas. Si la información discreta se transmite a una velocidad igual a N bps, el espectro consistirá en la componente de CD de frecuencia cero y en una secuencia infinita de armónicas con frecuencias iguales a f_0, $3f_0$, $5f_0$, $7f_0$, y así sucesivamente, donde $f_0 = N/2$. La frecuencia f_0 de este espectro se conoce como **frecuencia fundamental**.

Las amplitudes de estas armónicas disminuyen con mucha lentitud, con factores de 1/3, 1/5, 1/7 y así sucesivamente, de la amplitud de la armónica f_0 (figura 9.5*a*). Como resultado, para garantizar una transmisión de alta calidad, el espectro del código potencial requiere un ancho de banda amplio. Además, es necesario tomar en cuenta que en realidad el espectro de la señal cambia de manera constante en función de los datos que se transmiten a través de la línea. Por ejemplo, la transmisión de una secuencia larga de ceros y unos desplaza el espectro hacia las bajas frecuencias. En el caso extremo, cuando los datos que se transmiten están formados sólo de unos (o bien de ceros), el espectro consistirá en la armónica a la frecuencia cero. Cuando se transmitan unos y ceros alternados, no existirá componente de CD. Por lo tanto, el espectro de la señal resultante del código potencial en el curso de la transmisión de datos arbitrarios ocupará la banda de frecuencia que se extiende en el rango desde algún valor cercano a 0 Hz hasta una frecuencia casi igual a $7f_0$. Las armónicas a frecuencias mayores que $7f_0$ se pueden despreciar, pues su contribución a la señal resultante es mínima. Para el canal a una frecuencia de tonos, el límite superior para la codificación potencial se alcanza a una velocidad de transmisión de 971 bps, y un límite inferior no es aceptable a cualquier velocidad, porque el ancho de banda del canal comienza en 300 Hz. Como resultado, los códigos potenciales nunca se utilizan en los canales de tonos.

Cuando se usa AM, el espectro de la señal está formado por la onda senoidal a la frecuencia de la portadora (f_c), dos armónicas laterales $f_c + f_m$ y $f_c - f_m$, y las armónicas laterales $f_c + 3f_m$ y $f_c - 3f_m$. Aquí, f_m es la frecuencia a la que el parámetro de información de la senoidal cambia, el cual coincide con la velocidad de transmisión de datos cuando se usan dos niveles de amplitud (figura 9.5*b*). La frecuencia f_m determina el ancho de banda del enlace para el método de codificación seleccionado. A frecuencias de modulación bajas, el ancho del espectro de la señal también es bajo. De hecho, es igual a $2f_m$, siempre y cuando las armónicas a $3f_m$ que tengan menor cantidad de potencia se desprecien.

[3] Consulte cualquier libro en el campo de las matemáticas adoptado para la educación universitaria.

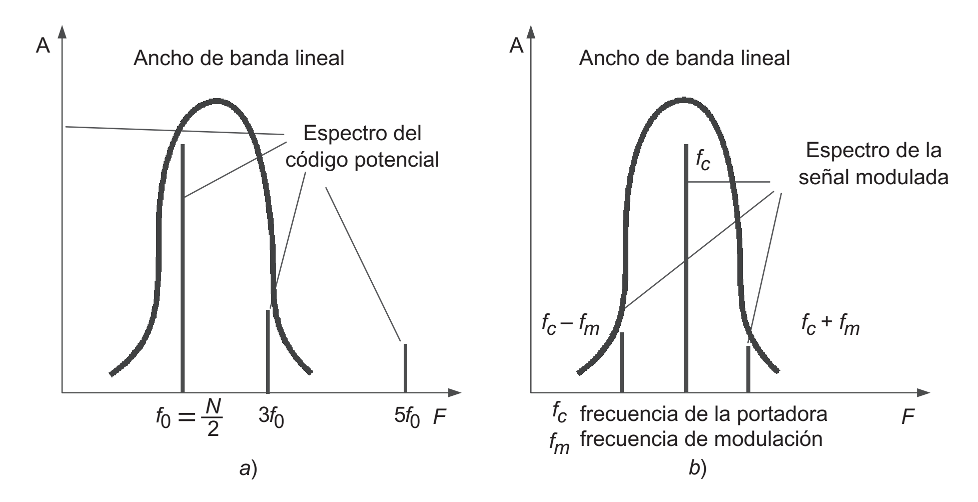


FIGURA 9.5 Espectros de señales que utilizan la codificación potencial y la modulación de amplitud.

Cuando se emplea la modulación de frecuencia y de fase, el espectro de la señal resulta más complejo que cuando se utiliza AM, ya que en este último caso existe un mayor número de armónicas laterales. Sin embargo, éstas se localizan en una posición simétrica respecto a la frecuencia portadora principal y sus amplitudes decrecen rápidamente.

9.3 DIGITALIZACIÓN DE SEÑALES ANALÓGICAS

PALABRAS CLAVE: digitalización, modulación por pulsos codificados (PCM), convertidor analógico a digital (ADC), convertidor digital a analógico (DAC), teoría del muestreo de señales de Nyquist-Kotelnikov, digitalización de la voz, y canal digital elemental.

En esta sección se estudiará la solución al problema inverso, es decir, la transmisión de información analógica en forma discreta.

En la práctica, este problema fue resuelto en la década de 1960 cuando las redes telefónicas comenzaron a transmitir voz como una secuencia de ceros y unos. La razón principal de esta conversión es la imposibilidad de mejorar la calidad de la transmisión de datos en forma analógica en el caso de que dichos unos y ceros fueran distorsionados durante la transmisión. La señal analógica por sí misma no proporciona signos de que se presentaron distorsiones o instrucciones acerca de cómo corregirlas. Esto sucede debido a que la señal puede tener cualquier forma de onda, incluida la que tiene registrada el receptor. Una mejora en la calidad de la línea (especialmente en lo relacionado con los prestadores de servicios regionales) requiere un gran esfuerzo y una inversión financiera considerable. Por lo tanto, el equipo analógico para la grabación y transmisión de voz se reemplazó por equipo digital. Esta técnica utiliza la **modulación de pulsos** de los procesos analógicos de la fuente, los cuales son continuos en el tiempo.

9.3.1 Modulación por pulsos codificados

Considere los principios de la modulación de pulsos del ejemplo de **modulación por pulsos codificados** (PCM), el cual se utiliza ampliamente en la telefonía digital.

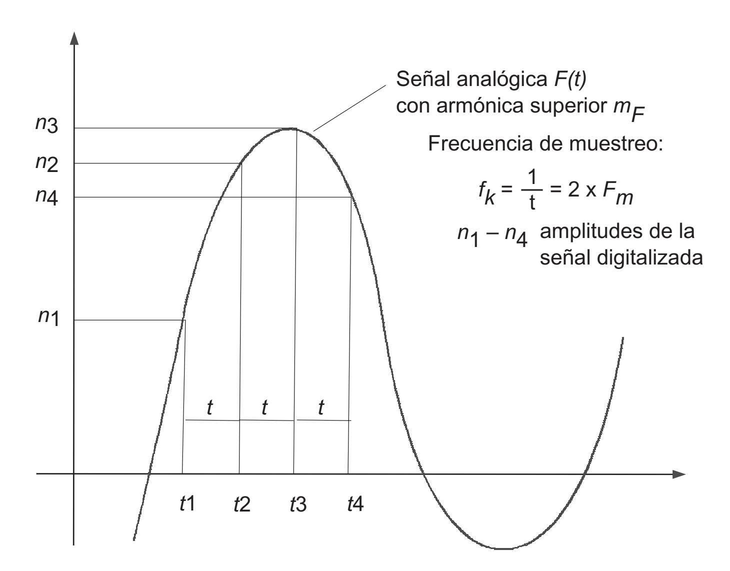


FIGURA 9.6 Modulación discreta de un proceso continuo.

Los métodos de modulación por pulsos se basan en el muestreo de procesos continuos tanto en amplitud como en tiempo (figura 9.6):

- La amplitud de la función de la fuente continua es medida con el periodo predefinido. Esto permite que el usuario pueda llevar a cabo el muestreo en el tiempo.
- Después, cada valor medido se representa mediante un número binario de longitud específica, el cual a su vez representa la cuantificación de los valores de la función —un conjunto continuo de valores posibles de amplitud es reemplazado por un conjunto discreto de sus valores—.

El dispositivo que lleva a cabo dicha función se conoce como **convertidor analógico a digital** (**ADC**). Después de esto, los valores muestreados son transmitidos mediante el uso de enlaces de comunicaciones en la forma de una secuencia de unos y ceros. Los mismos métodos de codificación se usan de manera simultánea, como en el caso de la transmisión de información discreta (por ejemplo, métodos basados en los códigos B8ZS o 2B1Q), los cuales se estudiarán más adelante en este capítulo.

En el extremo receptor de la línea, los códigos son transformados en secuencias de bits de la fuente y mediante el uso de un equipo especial conocido como **convertidor digital a analógico** (**DAC**) se lleva a cabo la demodulación de las amplitudes digitalizadas de una señal continua lo cual restablece la función de tiempo continuo de la fuente.

La modulación por pulsos se basa en la **teoría del muestreo de señales de Nyquist-Kotelnikov**. De acuerdo con dicha teoría, la función continua analógica transmitida en forma de secuencia de sus valores muestreados en el tiempo puede reconstruirse sin pérdidas, siempre y cuando la frecuencia de muestreo sea dos o más veces mayor que la frecuencia de la armónica más alta del espectro de la función de la fuente.

Si no se toma en cuenta esta condición, la función reconstruida será significativamente distinta de la función de la fuente.

La ventaja de los métodos digitales para la grabación, reproducción y transmisión de la información reside en la posibilidad de ejercer un control sobre la confiabilidad de los datos leídos provenientes del medio de transmisión o recibidos por la línea de comunicaciones.

Para este propósito, es posible utilizar los mismos métodos que se usaron para los datos de computadora, como el cálculo de la suma verificadora, la retransmisión de las tramas distorsionadas y el uso de códigos de autocorrección.

9.3.2 Digitalización de la voz

Para la transmisión de voz de alta calidad, la técnica PCM utiliza una frecuencia de muestreo de la amplitud de la oscilación del sonido de 8 000 Hz. Esto se debe a que en la telefonía analógica se seleccionó el rango de 300 a 3 400 Hz para la transmisión de voz. Dicho rango permite transmitir todas las armónicas significativas de la voz humana con una calidad aceptable. De acuerdo con el *teorema de Nyquist-Kotelnikov,* para la transmisión de voz de alta calidad basta seleccionar una frecuencia de muestreo que exceda la armónica de más alta frecuencia de la señal continua por al menos el doble (es decir, $2 \times 3\,400 = 6\,800$ Hz). La frecuencia de muestreo real seleccionada (8 000 Hz) proporciona un valor sobrado para efectos de calidad. Como regla general, el método PCM utiliza 7 u 8 bits de código para representar cada muestra. Estos valores corresponden al grado 127 o 256 de la señal sonora, que es suficiente para la transmisión de voz de alta calidad.

Cuando se emplea el método PCM, cada canal de voz requiere un ancho de banda de 56 Kbps o 64 Kbps, lo cual depende del número de bits utilizados para representar cada muestra. Si se usan 7 bits para este propósito, con la frecuencia de muestreo de 8 000 Hz, el resultado será:

$$8\,000 \times 7 = 56\,000 \text{ bps o } 56 \text{ Kbps}$$

De acuerdo con lo anterior, para 8 bits, el resultado será:

$$8\,000 \times 8 = 64\,000 \text{ bps o } 64 \text{ Kbps}$$

El canal digital de 64 Kbps, también conocido como **canal digital elemental,** es estándar.

La transmisión de una señal continua en forma discreta requiere que la red cumpla estrictamente con el requerimiento que prescribe que el intervalo entre dos muestras adyacentes debe ser de 125 μseg. Dicho intervalo corresponde a una frecuencia de muestreo de 8 000 Hz, lo cual significa que la red debe transmitir sincronizadamente los datos entre los nodos de la red. Si las muestras que llegan están fuera de sincronía, la señal de la fuente será recuperada de modo incorrecto, lo que provoca distorsión en la voz, imagen u otra información multimedia transmitida a través de redes digitales. Por lo tanto, una distorsión en la sincronización de 10 mseg dará como resultado el efecto eco, así como retardos entre muestras de 200 mseg o más y hará que el reconocimiento de las palabras individuales sea imposible. Al mismo tiempo, la pérdida de una sola muestra, prácticamente no tiene ningún efecto en la calidad de reproducción del sonido, siempre y cuando las demás muestras lleguen en sincronía. Esto se debe a la presencia de dispositivos emparejadores en los DAC, los cuales se basan en las propiedades inerciales de cualquier señal física. En este caso, la amplitud de las oscilaciones del sonido no puede cambiar inmediatamente en un valor significativo.

La calidad de la señal después del DAC está influida no sólo por la sincronización de las muestras que llegan a su entrada, sino también por el error de cuantificación de tales muestras. En la teoría de Nyquist-Kotelnikov, se supone que las amplitudes de la función se miden de manera precisa. Sin embargo, el uso de números binarios de ancho limitado distorsiona dichas amplitudes. De acuerdo con ello, la señal continua reconstruida también sufre distorsión. Este fenómeno se conoce como *ruido de cuantificación*.

9.4 MÉTODOS DE CODIFICACIÓN

PALABRAS CLAVE: sincronización del espectro de la señal, método de codificación, códigos autosincronizables, detección y corrección de datos distorsionados, código potencial sin retorno a cero (NRZ), inversión alternada de marcas bipolares (AMI), no retorno a cero con unos invertidos (NRZI), aleatorizador, desaleatorizador, código de pulsos bipolares, código Manchester, código potencial 2B1Q, códigos redundantes, código 4B/5B, B8ZS, HDB3, condensación de datos, condensación adaptable, empaquetamiento digital, codificación relativa, supresión de símbolos, códigos de longitud variable y algoritmo de Huffmann.

9.4.1 Selección de los métodos de codificación

Cuando se selecciona el método de codificación, se cumplen varios objetivos al mismo tiempo:

- Se minimiza el ancho espectral de la señal obtenida como resultado de la codificación.
- Se garantiza la sincronización entre el transmisor y el receptor.
- Se garantiza la inmunidad al ruido.
- Se garantiza la detección de errores en los bits y, si es posible, se corrigen dichos errores.
- Se minimiza la potencia del transmisor.

El espectro de la señal que se estudió en el capítulo 8 es una de las características más importantes del método de codificación. Un espectro más angosto de la señal permite una velocidad de transmisión de datos mayor en el mismo enlace (con el mismo ancho de banda). En el caso general, el espectro de la señal depende del método de codificación y de la frecuencia de reloj del transmisor. Por ejemplo, suponga que se han diseñado dos métodos de codificación, cada uno de los cuales transmite 1 bit de información durante cada señal de reloj (es decir, códigos binarios). Suponga también que, en el primer método, el ancho del espectro de la señal F es igual a la velocidad del reloj de la señal f (por ejemplo, $F = f$) y que el segundo método garantiza la dependencia siguiente: $F = 0.8f$. Entonces, con el mismo ancho de banda B, el primer método permite una velocidad de transmisión de datos de B bps, mientras que el segundo garantiza la transmisión de datos a una velocidad igual a $B/0.8 = 1.25B$ bps.

La sincronización del transmisor y el receptor es necesaria con el fin de garantizar que el receptor conozca cuándo debe leer nueva información de las líneas de comunicaciones. Cuando se transmite información discreta, el tiempo siempre se divide en ciclos de reloj de la misma duración y el receptor trata de leer cada nueva señal en la parte central de cada señal de reloj (es decir, sincroniza sus acciones con el transmisor).

El problema de la sincronización en las redes es más complejo que el intercambio de datos entre dispositivos ubicados entre sí a una distancia cercana (por ejemplo, entre varias unidades de una computadora o entre la computadora y la impresora local). En distancias más cortas, una configuración basada en una línea de comunicaciones independiente que transporte la señal de reloj (figura 9.7) funciona muy bien. De acuerdo con este método, la información se lee a partir de la línea de datos sólo cuando llegan los pulsos de reloj. En las redes, el uso de este método provoca dificultades debido a la no uniformidad de las características de los conductores en los cables. En largas distancias, la no uniformidad de la velocidad

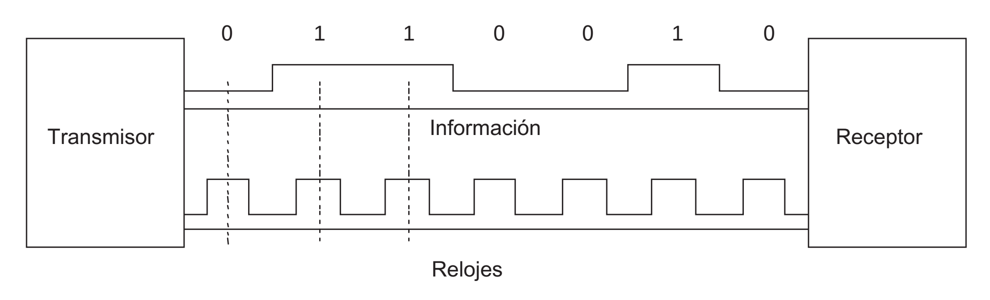


FIGURA 9.7 Sincronización del transmisor y el receptor a pequeñas distancias.

de propagación de las señales puede dar como resultado situaciones en las que el pulso de reloj llegue con mucha anticipación o muy tarde respecto a la señal de datos, lo cual provoca que se omitan bits o que se lean dos veces. Otra razón por la que los pulsos de reloj no se llevan por un cable independiente consiste en economizar los conductores de los cables.

En las redes, con el fin de resolver este problema se utilizan **códigos autosincronizables**. Las señales que transportan estos códigos llevan instrucciones para el receptor y especifican el momento en que es necesario reconocer el siguiente bit (o varios bits si el código está orientado hacia más de dos estados de la señal). Cualquier caída abrupta del nivel de la señal —el llamado **frente**— es un buen indicador para sincronizar el receptor con el transmisor.

Cuando se utilizan senoidales como señales portadoras, el código que resulta tiene la propiedad de autosincronización. Esto se debe a que el cambio en amplitud de la frecuencia portadora permite que el receptor detecte el comienzo del pulso de reloj siguiente.

La detección y corrección de datos distorsionados son operaciones difíciles de llevar a cabo con los medios proporcionados por la capa física. En consecuencia, esta tarea se realiza más a menudo con los protocolos de las capas superiores: de enlace de datos, de red, de transporte o de aplicación. Por otro lado, la detección de errores en el nivel de la capa física ahorra tiempo, pues el receptor no tiene que esperar hasta que se cargue toda la trama en la memoria, sino que la elimina inmediatamente en el momento de detectar bits erróneos en ella.

Los requerimientos de los métodos de codificación son contradictorios entre sí. Por lo tanto, cada uno de los métodos de codificación estudiados en este capítulo tiene ventajas y desventajas en comparación con otros métodos.

9.4.2 Código potencial de no retorno a cero

La figura 9.8*a* muestra el **método de codificación potencial** estudiado anteriormente, también conocido como **codificación sin retorno a cero (NRZ).** Este último nombre refleja que cuando se transmite una secuencia de unos, la señal no regresa a cero durante el ciclo de reloj, a diferencia de los demás métodos de codificación.

El método NRZ se caracteriza por poseer las ventajas siguientes:

- Facilidad de implementación.
- Buena capacidad para detectar errores (debido al uso de dos voltajes distintos).
- Espectro angosto (ya que la armónica fundamental f_0 es de baja frecuencia N/2 Hz, como se demostró en la sección titulada "Métodos combinados de modulación").

Por desgracia, este método no está libre de desventajas, entre las cuales las más importantes son las que siguen:

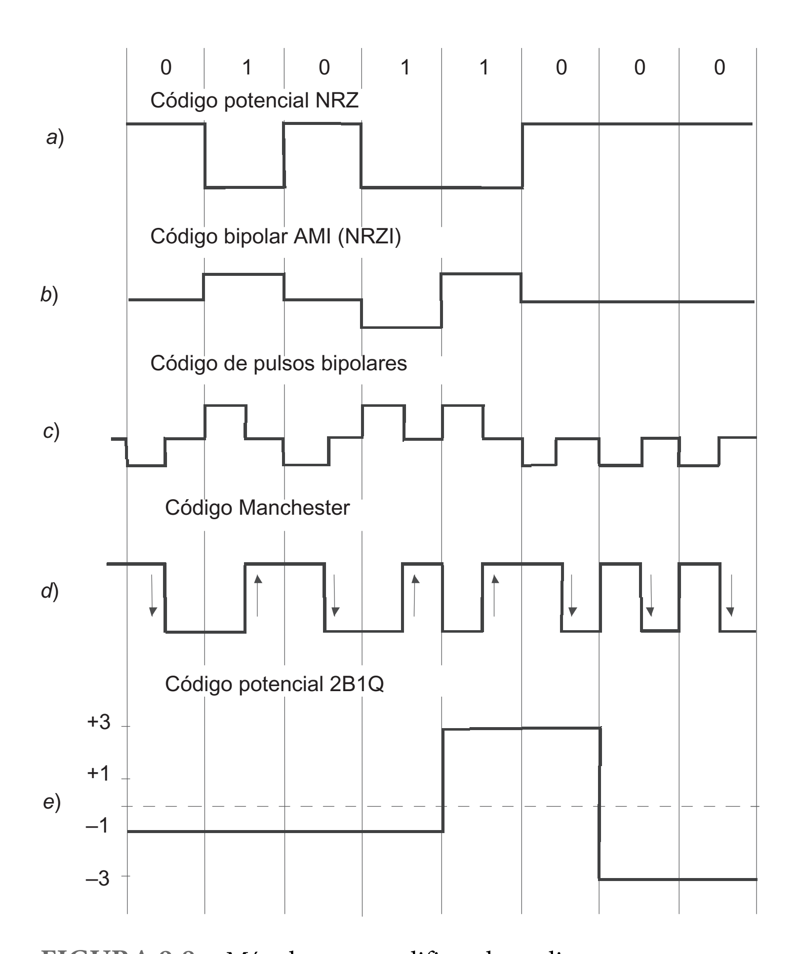


FIGURA 9.8 Métodos para codificar datos discretos.

- Falta de una propiedad de autosincronización. Incluso si el receptor estuviera equipado con un oscilador de reloj de alta precisión, los errores en la determinación de los datos que se van a leer aún son posibles, ya que las frecuencias de dos osciladores nunca son idénticas. Al mismo tiempo, recuerde que cuando se transmite una secuencia larga de unos o de ceros, la señal en la línea no cambia. Por ende, a una alta velocidad de transferencia de datos, siempre y cuando sean transmitidas largas secuencias de unos y ceros, aun una pequeña discrepancia en las frecuencias de reloj del transmisor o del receptor puede provocar un error igual a un ciclo de reloj. Como resultado, el receptor leerá un valor incorrecto de bits.
- La presencia de una componente constante de baja frecuencia, que se aproxima a cero cuando se transmiten largas secuencias de unos y ceros. Debido a esto, muchos enlaces de comunicaciones que no proporcionan una conexión galvánica directa entre el transmisor y el receptor no soportan este método de codificación. Como resultado, el código NRZ en su forma pura no se utiliza en las redes. No obstante, se usan las redes que emplean algunas de sus modificaciones. Éstas eliminan la pobre autosincronización del código NRZ y los problemas causados por la componente constante de baja frecuencia.

9.4.3 Codificación bipolar por inversión alternada de marcas

La **codificación bipolar por inversión alternada de marcas** (AMI) representa una de las modificaciones del método NRZ (figura 9.8*b*), el cual utiliza tres niveles de voltaje: negativo, cero y positivo. El voltaje cero se usa para codificar el cero binario y los voltajes binarios se codifican mediante pulsos diferentes de cero con polaridad alternada.

El código AMI elimina de forma parcial los problemas de componente de CD y la falta de bondades de autosincronización del código NRZ. Esto sucede cuando se transmiten largas cadenas de unos. En dichos casos, la señal de la línea es una secuencia de pulsos de polaridad alternada con el mismo espectro que el del código NRZ utilizado para transmitir unos y ceros alternados (es decir, sin componente de CD) y con la armónica principal igual a *N/2* Hz. En lo que se refiere a largas cadenas de ceros, éstas no son menos dañinas para el código AMI que para el código NRZ, debido a que en este caso la señal se degenera en un voltaje constante de amplitud igual a cero.

En general, para diferentes combinaciones de bits, el uso del código AMI resulta en espectros más angostos de la señal en comparación con el uso del código NRZ. En consecuencia, el código AMI incrementa la capacidad de la línea; por ejemplo, cuando se transmiten unos y ceros alternados, la armónica principal f_0 tiene una frecuencia igual a *N/4* Hz. El código AMI también proporciona algunas características para la detección de errores. Si por ejemplo, existe una violación de la estricta alternancia de la polaridad de la señal, ésta sirve como prueba de la presencia de un pulso falso o de la pérdida de un pulso correcto en la línea.

El código AMI utiliza tres niveles de señal en lugar de dos. El nivel de señal adicional requiere un aumento de la potencia del transmisor del orden de 3 dB aproximadamente con el fin de asegurar la misma confiabilidad en la recepción de bits. Esta desventaja es común a todos los códigos que manejan señales con varios estados.

9.4.4 Código de no retorno a cero con inversión de unos

Existe un código similar al AMI con sólo dos niveles de señal. Cuando se transmiten ceros, este código transmite el voltaje que se fijó en el ciclo de reloj anterior (es decir, no lo cambia) y cuando se transmite un uno, el código invierte el voltaje. Este código se conoce como de **no retorno a cero con unos invertidos** (*NRZI*). Su uso es conveniente cuando no se desea el tercer nivel de la señal, por ejemplo, en los cables de fibra óptica, donde únicamente dos estados de la señal se pueden detectar de manera estable: luz y oscuridad.

Se utilizan dos métodos para mejorar códigos potenciales similares al AMI y al NRZI. El primero de ellos se basa en la adición de bits redundantes que contienen unos lógicos al código fuente. En este caso se rompen las largas cadenas de ceros y el código obtiene propiedades de autosincronización para cualquier dato transmitido. La componente de CD también se elimina, lo cual significa que el espectro de la señal se hace más angosto. Sin embargo, este método reduce el ancho de banda efectivo en la línea, ya que los unos redundantes no llevan información alguna del usuario.

El otro método se basa en la mezcla de la información original para hacer que las probabilidades de que aparezcan ceros y unos en la línea sean aproximadamente iguales. Los dispositivos o unidades que llevan a cabo esta operación se conocen con el nombre de **aleatorizadores**. Durante el proceso de aleatorización, se utiliza un algoritmo bien conocido; por lo tanto, el receptor, una vez que ha recibido los datos binarios, los transfiere al **desaleatorizador**, el cual reconstruye la secuencia inicial de bits.

9.4.5 Código de pulsos bipolares

Además de los códigos de voltajes, las redes también utilizan códigos de pulsos en los que los datos se representan ya sea a través de un pulso completo o mediante una parte de éste: el frente. El **código de pulsos bipolares,** en el que un uno se representa mediante un pulso de una polaridad y un cero se representa mediante un pulso con la polaridad invertida (figura 9.8*c*), es el caso más simple de un código que implementa este método. Cada pulso tiene una duración de medio ciclo de reloj. Dicho código está caracterizado por algunas propiedades de autosincronización excelentes. Sin embargo, la componente de CD debe estar presente, por ejemplo: cuando se transmiten largas cadenas de bits compuestas por unos y ceros. Además, el espectro de este código es más ancho que el espectro de los códigos potenciales. Por ejemplo, si se transmiten sólo ceros o sólo unos, la frecuencia de la armónica principal será siempre igual a *N* Hz, la cual es dos veces mayor que la frecuencia de la armónica principal del código NRZ y cuatro veces mayor que la frecuencia de la armónica principal del código AMI cuando se transmiten unos y ceros alternados. Debido al excesivo ancho del espectro, rara vez se utiliza un código de pulsos bipolares.

9.4.6 Código Manchester

Hasta fechas recientes, el **código Manchester** fue el método de codificación más popular utilizado en las LAN (figura 9.8*d*). Este código se utiliza en tecnologías como Ethernet y Token Ring.

En el código Manchester, la transición de voltaje (es decir, frente del pulso) se usa para codificar unos y ceros. Cuando se emplea este método de codificación, cada ciclo de reloj se divide en dos partes. La información se codifica mediante transiciones de voltaje que se presentan en el punto medio de cada ciclo de reloj. El uno se codifica mediante la transición del nivel de señal bajo al alto, mientras que un cero se representa por la caída de voltaje. Al comienzo de cada ciclo de reloj, puede presentarse una transición en la señal de servicio si es que es necesario transmitir varios unos y ceros uno después del otro. Como la transmisión de un solo bit de datos requiere que la señal cambie al menos una vez por señal de reloj, el código Manchester tiene muy buenas características de autosincronización. El ancho de banda de dicho código es más angosto que el código de pulsos bipolares. Además, el código Manchester no tiene componente de CD y la armónica principal en el peor caso (es decir, cuando se transmite una cadena larga de unos y ceros) tiene una frecuencia de *N* Hz. En el mejor de los casos (cuando se transmiten unos y ceros alternados), la frecuencia de la armónica principal será de *N*/2 Hz, lo cual también sucede con los códigos AMI y NRZ. En promedio, el ancho de banda del código Manchester es 1.5 veces más angosto que el del código de pulsos bipolares y la frecuencia de la armónica principal fluctúa alrededor de 3*N*/4. El código Manchester tiene otra ventaja cuando se compara con el código de pulsos bipolares, ya que este último utiliza tres niveles de señal y el código Manchester usa solamente dos.

9.4.7 Código potencial 2B1Q

La figura 9.8*e* muestra un código potencial con cuatro niveles de señal utilizados para codificar los datos. Es el código **2B1Q**, cuyo nombre refleja su idea principal: cada 2 bits (2B o dos binario) se transmiten en cada reloj mediante una señal que tiene cuatro estados (1Q quiere decir cuaternaria). El par de bits iguales a 00 se codifica mediante un potencial igual a –2.5V, 01 por un potencial igual a –0.833 V, 11 por un potencial de +0.833 V y el 10 por un potencial igual a +2.5 V.

Cuando se utiliza este método de codificación, es necesario realizar pasos adicionales para eliminar largas cadenas de pares de bits idénticos, ya que en este caso la señal se convierte en la componente de CD. Cuando los bits se alternan de manera aleatoria, el espectro de la señal es dos veces más angosto que aquel del código NRZ, pues para la misma velocidad de transmisión, la duración del reloj aumenta dos veces. Por lo tanto, mediante el uso del código 2B1Q es posible transmitir datos a través de la misma línea a una velocidad del doble de la de los códigos AMI y NRZI. Sin embargo, para implementar este código, la potencia del transmisor debe incrementarse para garantizar que el receptor pueda reconocer claramente cuatro niveles de señal, a pesar de la presencia de ruido de fondo.

Los códigos redundantes y la aleatorización se utilizan con la finalidad de mejorar los códigos potenciales como el AMI, NRZI y 2Q1B.

9.4.8 Códigos redundantes

Los **códigos redundantes** se basan en la segmentación de la secuencia de bits fuente en porciones, llamadas por lo general *símbolos*. Después, cada símbolo fuente se reemplaza por otro con un número mayor de bits.

Por ejemplo, un código lógico como el **4B/5B** utilizado en las tecnologías FDDI y Fast Ethernet reemplaza los símbolos fuente que tengan una longitud de 4 bits por otros que tengan una longitud de 5 bits. Como los símbolos resultantes contienen bits redundantes, el número común de combinaciones de bits entre ellos es mayor que el de los caracteres de la fuente. Por ejemplo, en el código 4B/5B, los caracteres resultantes pueden contener combinaciones de 32 bits y los iniciales tienen 16 combinaciones (tabla 9.1). Por lo tanto, es posible seleccionar 16 de tales combinaciones del código resultante (las que no contengan un gran número de ceros) y considerar las demás combinaciones como *violaciones al código.* Además de eliminar la componente de CD y garantizar la propiedad de autosincronización del código, los bits redundantes permiten que el receptor detecte bits distorsionados. Si el receptor encuentra una violación al código, se presenta una distorsión de la señal en la línea.

TABLA 9.1 Correspondencia de la fuente y los códigos resultantes del código 4B/5B

Código fuente	Código resultante	Código fuente	Código resultante
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Después de segmentar, el código resultante 4B/5B se transmite a través de la línea utilizando uno de los métodos de la codificación potencial, la cual es sensible sólo a las cadenas largas de ceros. Los símbolos de cinco bits del código 4B/5B garantizan que no más de tres ceros sucesivos puedan encontrarse en la línea para cualquier combinación de símbolos de código resultante.

NOTA *La letra B en el código 4B/5B quiere decir binario y significa que la señal elemental tiene dos estados. Existen también códigos con tres estados de señal. Por ejemplo, el 8B/6T codifica 8 bits de datos con seis símbolos ternarios, lo cual significa que cada uno de estos símbolos tiene tres estados. La redundancia del código 8B/6T es mayor que la del 4B/5B, pues existen* $3^6 = 729$ *caracteres resultantes para codificar* $2^8 = 256$ *códigos fuente.*

El uso de la tabla para la conversión de códigos es una tarea sencilla. Por lo tanto, este método no hace más complejos los adaptadores de red y las unidades de interfaz de los switches y ruteadores.

Para garantizar un ancho de banda específico en la línea, el transmisor que utiliza el código debe trabajar a una frecuencia de reloj aumentada. Por lo tanto, para transmitir códigos 4B/5B a una velocidad de 100 Mbps, el transmisor debe trabajar a una frecuencia de reloj de 125 MHz. Al mismo tiempo, el espectro de la señal de la línea se ensancha en comparación cuando se transmite un código sin redundancia a través de la línea. Sin embargo, el espectro del código potencial redundante demuestra ser más angosto que el espectro del código Manchester. Este hecho justifica una etapa adicional de codificación lógica, así como la operación del transmisor y el receptor a una frecuencia de reloj incrementada.

9.4.9 Aleatorización

Los métodos de *aleatorización* consisten en el cálculo bit por bit del código resultante basado en los bits del código inicial y los bits del código resultante que se obtuvieron durante los ciclos de reloj anteriores. Por ejemplo, un aleatorizador puede implementar la relación siguiente:

$$B_i = A_i B_{i-3} B_{i-5} \tag{9.1}$$

Aquí, B_i es el dígito binario del código resultante obtenido en el ciclo de reloj i-ésimo de la operación del aleatorizador; A_i es el dígito binario del código fuente que llega del i-ésimo ciclo de reloj a la entrada del aleatorizador, y B_{i-3} y B_{i-5} son dígitos binarios del código resultante que se obtuvo en los ciclos de reloj anteriores a la operación de aleatorización (tres y cinco ciclos de reloj antes del actual, respectivamente) y unidos mediante la operación lógica OR exclusiva (XOR) (por ejemplo, adición módulo 2).

Por ejemplo, si la secuencia fuente es 110110000001, el aleatorizador producirá el código siguiente (los primeros tres dígitos del código resultante coincidirán con el código fuente, pues los dígitos anteriores requeridos todavía no están disponibles):

$B_1 = A_1 = 1$

$B_2 = A_2 = 1$

$B_3 = A_3 = 0$

$B_4 = A_4\ B_1 = 1\ 1 = 0$

$B_5 = A_5\ B_2 = 1\ 1 = 0$

$B_6 = A_6\ B_3\ B_1 = 0\ 0\ 1 = 1$

$B_7 = A_7\, B_4\, B_2 = 0\ 0\ 1 = 1$

$B_8 = A_8\, B_5\, B_3 = 0\ 0\ 0 = 0$

$B_9 = A_9\, B_6\, B_4 = 0\ 1\ 0 = 1$

$B_{10} = A_{10}\, B_7\, B_5 = 0\ 1\ 0 = 1$

$B_{11} = A_{11}\, B_8\, B_6 = 0\ 0\ 1 = 1$

$B_{12} = A_{12}\, B_9\, B_7 = 1\ 1\ 1 = 1$

Por lo tanto, la siguiente cadena aparecerá a la salida del aleatorizador: 110001101111, la cual no contiene la subcadena que tiene los seis ceros sucesivos que estaban en el código fuente.

Después de recibir la cadena resultante, el receptor la pasa al desaleatorizador, el cual restablece la secuencia inicial con base en la relación inversa:

$$C_i = B_i\, B_{i-3}\, B_{i-5} = (A_i\, B_{i-3}\, B_{i-5})\, B_{i-3}\, B_{i-5} = A_i \qquad (9.2)$$

Los algoritmos de aleatorización difieren en el número de operandos que produce el dígito del código resultante y en el corrimiento entre ellos. Por ejemplo, en las redes ISDN, el algoritmo de aleatorización utiliza una transformación con corrimientos de 5 y 23 posiciones cuando se transmiten datos de la red al abonado; cuando se transmiten datos del abonado a la red, la conversión por parte del aleatorizador utiliza corrimientos de 18 y 23 posiciones.

Existen métodos más sencillos para eliminar las cadenas de unos sucesivos, también clasificados como métodos de aleatorización.

Para mejorar el código AMI bipolar, se utilizan dos métodos basados en la distorsión artificial de cadenas de ceros mediante caracteres no válidos.

La figura 9.9 muestra el uso del código bipolar con sustitución de ocho ceros (**B8ZS**) y el código bipolar de tres ceros de alta densidad (**HDB3**) para corregir el código AMI. El código fuente consiste en dos largas cadenas de ceros; en el primer caso hay ocho ceros y en el segundo cinco.

El código B8ZS corrige solamente cadenas que consisten en ocho ceros consecutivos. Para lograr esto, el código inserta cinco dígitos después de los primeros tres ceros: *V*–1*–0–*V*–1*.

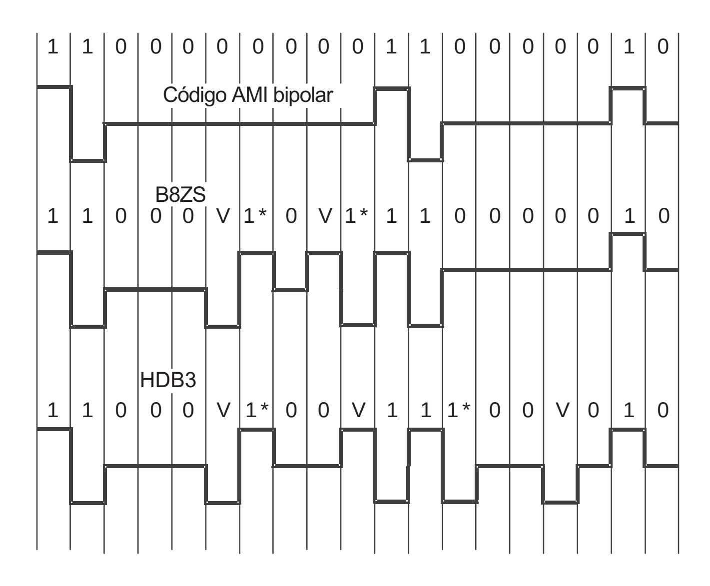


FIGURA 9.9 Códigos B8ZS y HDB3.

Aquí, *V* quiere decir que la señal uno de polaridad no es válida para el ciclo de reloj actual (es decir, la señal que no cambia la polaridad del "uno" anterior), mientras que *1** quiere decir que la señal "uno" de polaridad es correcta (el asterisco especifica que en el código fuente no había un cero en este reloj). Como resultado, durante ocho pulsos de reloj, el receptor detecta dos distorsiones. Es extremadamente poco probable que esto hubiera pasado debido al ruido en la línea u otra falla en la transmisión. Por lo tanto, el receptor considera dichas violaciones como la codificación de la secuencia que comprende ocho ceros consecutivos. Después de recibir esta secuencia, el receptor la reemplaza con los ocho ceros iniciales. El código B8ZS está construido de tal forma que su componente de CD es igual a cero aun si tiene cualquier secuencia de dígitos binarios.

El código HDB3 corrige cuatro ceros consecutivos en la secuencia inicial. Las reglas para formar el código HDB3 son más complejas que las del código B8ZS. Cada grupo formado por cuatro ceros es reemplazado por cuatro señales, donde existe una señal *V*. Para eliminar la componente de CD, la polaridad de la señal *V* es alternada en los reemplazos consecutivos. Además de ello se utilizan dos patrones de códigos de cuatro relojes para el reemplazo. Si antes del reemplazo el código fuente contenía un número impar de unos, se usa el patrón 000*V*, y si el número de unos era par, se emplea el patrón 1*00*V* como reemplazo.

Los códigos potenciales mejorados tienen un ancho de banda muy angosto para cualquier secuencia de unos y ceros que puedan encontrarse en los datos transmitidos. La figura 9.10 muestra los espectros de señal de diferentes códigos que se obtienen cuando se transmiten datos en forma arbitraria, donde cualquier combinación de unos y ceros es igualmente probable que pueda ser encontrada en el código fuente. Cuando se construyen gráficas, para calcular el espectro se promedian todos los conjuntos posibles de secuencias iniciales. Como es natural, los códigos resultantes pueden tener diferentes distribuciones de unos y ceros. En la figura se observa que el código potencial NRZ tiene un buen espectro sólo con una desventaja: tiene una componente de CD. Los códigos obtenidos a partir del código potencial mediante la codificación lógica tienen un espectro más angosto que el código Manchester. Esto es válido aun para frecuencias de reloj incrementadas. (En la figura 9.10, el espectro del código 4B/5B podría coincidir aproximadamente con el código B8ZS en lugar de ser

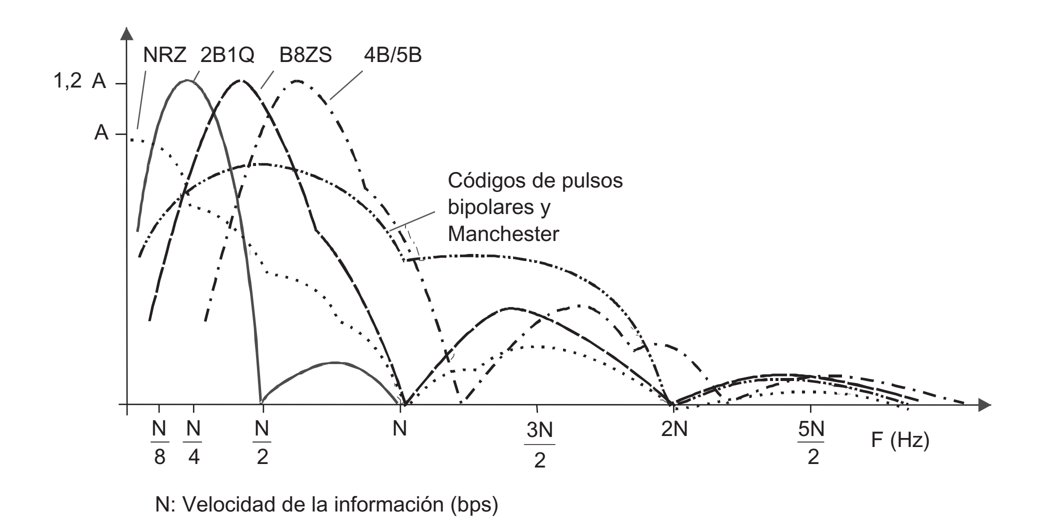


FIGURA 9.10 Espectros de códigos potenciales y de pulsos.

desplazado a la zona de frecuencias mayores, pues su frecuencia de reloj aumenta en una cuarta parte de la correspondiente a los demás códigos.) Esto explica por qué los códigos potenciales redundantes y aleatorizados se utilizan en las tecnologías actuales de forma similar a FDDI, Fast Ethernet, Gigabit Ethernet, ISDN, etc., en lugar del código Manchester o el código de pulsos bipolares.

9.4.10 Compresión de datos

La **compresión de datos** es una técnica que reduce el volumen de información original sin perder su contenido. Dicha compresión se utiliza en la conectividad de redes para reducir el tiempo de transmisión. En general, los beneficios resultan en la reducción del tiempo de transmisión, debido a que la compresión de datos solamente se observa en enlaces lentos. Esto sucede debido a que la instancia que transmite consume un tiempo adicional comprimiendo los datos y la instancia receptora tiene que esperar un tiempo igual para descomprimirlos. Este umbral de la velocidad de transmisión es aproximadamente de 64 Kbps en los equipos modernos. La mayoría de las herramientas de software y hardware pueden llevar a cabo la *compresión dinámica de datos* en contraste con la compresión estática, donde los datos por transmitir se comprimen con antelación (por ejemplo, si se utilizan aplicaciones muy conocidas para archivos, como el WinZip) y solamente hasta entonces se envían hacia la red.

En la práctica se pueden emplear varios algoritmos de compresión, cada uno de los cuales es aplicable a un tipo específico de datos. Algunos módems (conocidos como inteligentes) brindan la compresión **adaptable**. Cuando se utiliza la compresión adaptable, el módem selecciona el algoritmo de compresión específico en función de los datos que se transmiten. A continuación se estudiarán varios algoritmos de compresión comunes.

Empaquetamiento decimal significa que los datos abarcan solamente números y será posible lograr ahorros significativos si se reduce el número de bits utilizados para codificar un dígito. Mediante el uso de la codificación binaria simple de dígitos decimales en lugar del código ASCII se reducirá el número de bits utilizados para representar un dígito del 7 al 4. Tres de los bits más significativos de los códigos ASCII correspondientes a los números decimales contienen la combinación 011. Si todos los datos en la trama de información contienen sólo dígitos decimales, será posible reducir significativamente la longitud de la trama si se coloca un carácter de control apropiado en el encabezado de la trama.

La **codificación relativa** representa una opción al empaquetamiento decimal cuando se transmiten datos numéricos con pequeñas desviaciones entre dígitos consecutivos. En este caso, es posible transmitir únicamente estas desviaciones junto con el valor de referencia conocido. En particular, este método se utiliza con el método de codificación digital de voz ADPCM, donde en cada reloj se transmite solamente la diferencia entre dos mediciones de voz consecutivas.

La **supresión de símbolos** puede explicarse como sigue: con mucha frecuencia, los datos que se transmiten contienen un gran número de bytes duplicados. Por ejemplo, cuando se transmiten imágenes en blanco y negro, las superficies negras generarán una gran cantidad de valores iguales a cero y las regiones con imágenes iluminadas al máximo contendrán múltiples bytes formados solamente por unos. El transmisor explora la secuencia de bytes que son transmitidos y, si se detecta la secuencia que contiene tres o más bytes idénticos, se reemplaza por una secuencia especial de 3 bytes que especifica el valor del byte, detecta el número de valores duplicados y marca el punto de comienzo de la secuencia con un carácter de control especial.

Los métodos de codificación de **códigos de longitud variable** se basan en el hecho de que no todos los caracteres contenidos en la trama que se transmite se encuentran en la misma frecuencia. Debido a esto, muchos métodos de codificación reemplazan los códigos de los caracteres más comúnmente encontrados por códigos más cortos. Los códigos de caracteres que se hallan muy rara vez son reemplazados por códigos más largos. Dicha codificación también se conoce con el nombre de codificación estática. Debido a que los símbolos tienen diferentes longitudes, sólo es posible utilizar la transmisión orientada al bit para transmitir tramas.

Cuando se usa la **codificación estática**, los códigos se seleccionan con el fin de determinar sin ambigüedades la correspondencia de cierta porción de bits con un símbolo específico o con una combinación de bits no válida cuando se analiza una secuencia de bits. Si una combinación de bits específica representa una violación, es necesario agregar un bit más a esta secuencia y repetir el análisis. Por ejemplo, si el código 1 se selecciona para designar el carácter más frecuente —E, el cual comprende 1 bit—, el valor 0 del código de un solo bit representará una violación. De otra forma, el usuario podrá codificar sólo dos caracteres. Para otro carácter frecuente —T— es posible utilizar el código 01 y considerar el 00 como una violación al código. Entonces, para el carácter A es posible seleccionar el código 001 y el 0001 puede seleccionarse para el carácter I. La utilización de códigos de longitud variable es más eficaz cuando la irregularidad de la distribución en frecuencia de los símbolos transmitidos es significativa. Éste es el caso con largas secuencias de texto. Por el contrario, este método es ineficaz cuando se transmiten datos binarios, como el código fuente de un programa, ya que los códigos de 8 bits están distribuidos de una forma casi uniforme.

Uno de los algoritmos más comunes con base en el cual se construyen los códigos de longitud variable es el **algoritmo de Huffmann,** el cual permite formar códigos de manera automática a partir de frecuencias conocidas de las ocurrencias de caracteres. Existen modificaciones adaptativas al método de Huffmann que permiten que el árbol del código se pueda construir a medida que se reciban los datos de la fuente.

Muchos equipos de comunicaciones, como los módems, puentes, switches y ruteadores soportan protocolos de compresión dinámica que permiten reducir el volumen de información transmitida de cuatro o hasta ocho veces. En estos casos, el protocolo garantiza una relación de compresión de 1:4 o de 1:8. Existen protocolos de compresión estándares, como el V.42bis, así como un gran número de protocolos propietarios. La relación de compresión real depende del tipo de datos que se vayan a transmitir. Por ejemplo, los datos de gráficas y texto usualmente se comprimen muy bien, pero la compresión del código fuente de un programa es menos eficaz.

9.5 DETECCIÓN Y CORRECCIÓN DE ERRORES

PALABRAS CLAVE: códigos de autocorrección, suma verificadora, secuencia de verificación de trama (FCS), control de paridad, control de paridad vertical y horizontal, verificación de redundancia cíclica (CRC), corrección de errores hacia delante (FEC), distancia de Hamming y códigos Hamming.

La transmisión confiable de información puede garantizarse mediante el uso de varios métodos. En el capítulo 6 se analizaron los principios de operación de los protocolos responsables de asegurar la confiabilidad por medio de la retransmisión de paquetes perdidos o dañados. Dichos protocolos se basan en la habilidad del receptor para detectar la información dañada en el paquete recibido. Con este propósito, se utilizan métodos especiales

para detectar errores. Existe otro método para garantizar la confiabilidad: el uso de códigos de autocorrección. Dichos códigos, además de detectar errores en la trama recibida, son capaces de corregirlos. Este último método es mucho más rápido que la retransmisión de la trama.

9.5.1 Técnica de detección de errores

Los métodos para detectar errores se basan en la transmisión de información redundante dentro de bloques de datos. Mediante el uso de esta información es posible determinar si la información recibida resulta correcta con cierto nivel de probabilidad. En las redes de conmutación de paquetes, el PDU de cualquier capa puede servir como tal unidad de información: tramas, paquetes o segmentos. Para distinguirlas, puede considerarse que son tramas de control.

La información de servicio redundante se conoce como **suma verificadora** o **secuencia de verificación de tramas** (**FCS**). La suma verificadora se calcula en función de la información principal, no necesariamente con sólo sumar. La entidad receptora recalcula la suma verificadora de la trama de acuerdo con el algoritmo conocido y, en caso de que coincida con la suma verificadora calculada por la instancia transmisora, concluye que los datos fueron transmitidos correctamente a través de la red. El código que contiene los bits redundantes, además de la información del origen, a menudo se llama *palabra código*.

Existen varios algoritmos comunes para calcular la suma verificadora que difieren en sus niveles de complejidad para detectar errores en los datos.

El **control de paridad** es el método más simple para controlar datos, así como es el algoritmo para el control de errores menos poderoso, pues su uso solamente permite detectar errores aislados en los datos que se verifican. Este método consiste en la suma módulo 2 de todos los bits que constituyen la información que se controla. Por ejemplo, si el byte es igual a 100101011, la suma verificadora será igual a 1. Como se observa fácilmente, en la información que contiene un número de unos impar, la verificación de paridad siempre da 1, mientras que para un número par de unos da 0. El resultado del cálculo de la suma verificadora es un bit de datos redundante que se envía junto con la información que se controla. Si durante la transmisión cualquier bit de la fuente de datos (o suma verificadora) se daña, el resultado del cálculo de la suma verificadora será distinto de la calculada al inicio, lo cual sirve como evidencia de que existe un error. Sin embargo, un doble error como 110101010 no se notará y se considerará de manera equivocada que los datos están correctos. Por lo tanto, el control de paridad suele aplicarse a pequeñas porciones de datos (1 byte como regla), lo cual genera un coeficiente de redundancia igual a 1/8. Este método se utiliza muy rara vez en las redes de computadoras debido a la redundancia significativa que éste posee, así como a las insuficientes capacidades de diagnóstico que tiene. El control de paridad cuenta con dos variantes: control con paridad par cuando el número de unos se complementa a un número par (como en el ejemplo anterior) y control con paridad impar cuando el resultado de un cálculo es invertido, y complementa el número de unos a un número impar.

El **control de paridad vertical y horizontal** es una modificación del método que se acaba de describir. Su diferencia reside en que los datos iniciales se consideran una matriz, cuyos renglones conforman los bytes de datos. El bit de control se calcula de manera separada por fila y por columna. Este método permite detectar gran parte de los errores dobles. No obstante, su redundancia es mucho más significativa cuando se compara con el método anterior. En la práctica, este método nunca se utiliza para transmitir información a través de una red.

La **verificación de redundancia cíclica** (**CRC**) es en la actualidad el método más conocido para controlar errores en las redes de computadoras. Este método no está limitado a las redes; por ejemplo, se utiliza activamente cuando se escriben datos en discos duros y flexibles.

Asimismo, dicho método estima que la fuente de datos es un número binario de muchos bits. Por ejemplo, la trama Ethernet que comprende 1 024 bytes se considera un solo número de 8 192 bits. El residuo de la división de este número entre un divisor conocido, *R*, se considera información de control. Como regla, se selecciona un número de 17 bits o de 33 bits como divisor con el fin de garantizar que el residuo de la división tenga una longitud de 16 bits (2 bytes) o 32 bits (4 bytes). Esto implica tomar en cuenta que el residuo es siempre 1 bit más corto que el dividendo. Cuando se recibe la trama de datos, el residuo de la división entre el mismo divisor *R*, se calcula una vez más. Sin embargo, en este caso, la suma verificadora dentro de la trama se agrega a los datos de ella. Si el residuo dividido entre *R* es igual a cero, se puede concluir que no ha habido errores en la trama recibida. Si no es así, se considera que la trama contiene errores.

Dicho método es mucho más complejo a pesar de que sus características de diagnóstico son muchos mayores que las de los métodos para controlar la paridad. El método CRC detecta todos los errores individuales, los dobles errores y los errores en un número impar de bits. El nivel de redundancia de este método no es muy grande. Por ejemplo, para una trama Ethernet con un tamaño de 1 024 bytes, la información de control tiene una longitud de 4 bytes, lo cual significa sólo el 0.4%.

9.5.2 Corrección de errores

La técnica de codificación que permite al receptor no solamente detectar errores en los datos recibidos sino también corregirlos se conoce como **corrección de errores hacia delante** (FEC). Los códigos garantizados por este FEC requieren un grado de redundancia de los datos transmitidos mayor que los códigos que solamente detectan errores.

Cuando se utiliza cualquier código redundante, no todas las combinaciones de código están permitidas. Por ejemplo, el control de paridad permite solamente la mitad de los códigos. Si el lector controla tres bits de información, se permitirán los siguientes códigos de 4 bits que complementan a un número impar de unos:

000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0

Los anteriores son solamente ocho códigos de un total de 16.

Con el fin de evaluar el número de bits auxiliares que se requieren para la corrección de errores, es necesario conocer la llamada **distancia de Hamming** entre las combinaciones de códigos permitidas. Dicha distancia es el número mínimo de bits por el cual difiere cualquier par de códigos permitidos. En los métodos para controlar la paridad, la distancia de Hamming es de 2 bits.

Es posible demostrar que si se diseña un código redundante con distancia de Hamming igual a n, dicho código podrá ser capaz de detectar $(n-1)$ errores y de corregir $(n-1)/2$ errores. Puesto que los códigos para el control de paridad tienen una distancia de 2 bits, éstos solamente pueden detectar errores individuales, sin embargo, no pueden corregir ningún error.

Los **códigos Hamming** detectan y corrigen errores aislados de manera eficaz (es decir, bits individuales erróneos separados por una gran cantidad de bits correctos). Sin embargo, si se encuentra una larga secuencia de bits erróneos (también conocidas como ráfagas de errores), el uso de los códigos Hamming no será apropiado.

Las situaciones en las que se encuentran ráfagas de errores son típicas de los canales inalámbricos. En este caso, se utilizan los *métodos de codificación convolucionales*. Dado que para detectar el código correcto más probable este método utiliza el diagrama de trellis, tales códigos se llaman *códigos trellis*, los cuales se utilizan no sólo en canales inalámbricos, sino también en módems.

9.6 MULTIPLEXAJE Y CONMUTACIÓN

PALABRAS CLAVE: multiplexaje por división de frecuencia (FDM), multiplexaje por división de longitud de onda (WDM), multiplexaje por división de tiempo (TDM), acceso múltiple por división de código (CDMA), sub-banda, WDM denso (DWDM), modo TDM asíncrono, modo TDM, ranura de tiempo, multiplexor, tramas fundamentales estándar T1, demultiplexor, modo de transferencia sincrónica conmutada (STM), TDM estadístico (STDM), modo de transferencia asincrónica (ATM), dúplex por división de frecuencia (FDD) y división dúplex (TDD).

Los métodos de codificación y corrección de errores permiten a los usuarios crear un enlace a través de un medio de transmisión, como en los alambres de cobre del cable. Sin embargo, esto no es suficiente para conectar de manera eficaz a los usuarios de una red. En este enlace, es necesario crear canales individuales que se utilizarán para conmutar los flujos de información de los usuarios. Para diseñar un canal de usuario, los switches de las redes de transmisión deben ser capaces de soportar algunas técnicas de multiplexaje y conmutación. Los métodos de conmutación están relacionados estrechamente con el método de multiplexaje empleado para crear canales; por lo tanto, ambos se estudiarán es este capítulo.

Por el momento, los métodos siguientes se utilizan para el multiplexaje de los canales de usuario:

- Multiplexaje por división de frecuencia (FDM).
- Multiplexaje por división de longitud de onda (WDM).
- Multiplexaje por división de tiempo (TDM).
- Acceso múltiple por división de código (CDMA).

El multiplexaje TDM se utiliza con las técnicas de conmutación de circuitos y de paquetes. Los métodos como FDM, WDM y CDMA son aplicables solamente a la técnica de conmutación de circuitos. El método CDMA se usa sólo con el método de espectro disperso y se analizará con más detalle en el siguiente capítulo, el cual está dedicado a la transmisión inalámbrica.

9.6.1 Conmutación de circuitos basada en FDM y WDM

La **técnica FDM** se diseñó para las redes telefónicas, aunque es aplicable también a otros tipos de redes. Algunos ejemplos son las redes de transmisión (canales de microondas) y las redes de televisión por cable.

La idea principal en la que se apoya este método consiste en asignar a cada banda de frecuencia de las diferentes conexiones un espacio dentro del ancho de banda total del enlace.

Con base en dicha sub-banda, se crea el **canal**. Los datos transmitidos a través del canal son modulados mediante el uso de uno de los métodos descritos con anterioridad y que hacen uso de la frecuencia de la portadora que pertenece a la banda del canal. Para realizar el multiplexaje se emplea el mezclador de frecuencias y el demultiplexaje se logra al usar un filtro de banda angosta con un ancho igual al de la banda del canal.

En seguida se analizarán algunas características específicas de este tipo de multiplexaje en las redes telefónicas.

Las señales fuente que provienen de los abonados de la red telefónica se alimentan a las entradas del switch FDM, el cual desplaza la frecuencia de cada canal a la banda asignada a éste mediante la modulación de la frecuencia específica de la portadora. Para evitar el

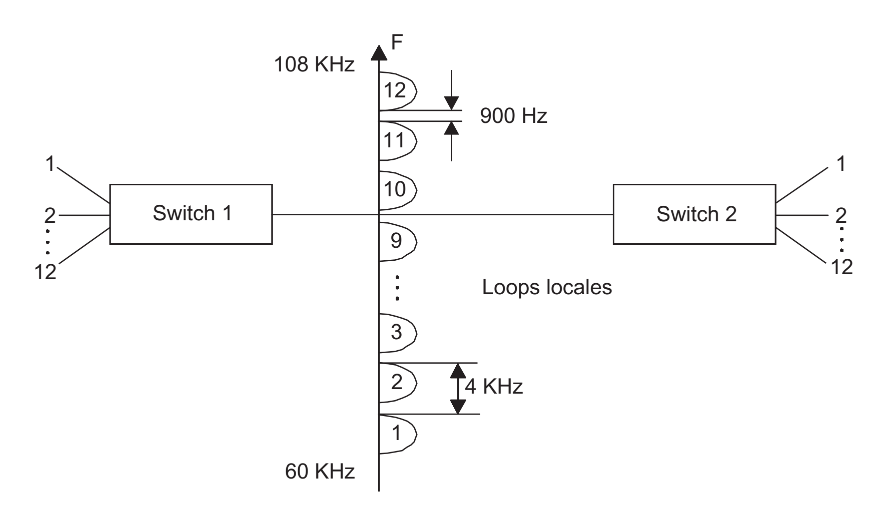


FIGURA 9.11 Conmutación con base en FDM.

mezclado de las componentes de baja frecuencia de los distintos canales, a las bandas se les asigna 4KHz en vez de 3.1 KHz, lo que permite que exista un intervalo de 900 Hz especial entre ellos (figura 9.11). El enlace entre dos switches FDM transmite señales de forma simultánea a todos los canales de los abonados, aunque cada uno de ellos toma su propia banda de frecuencia. Dicho enlace se llama *enlace multiplexado*.

Un switch FDM de salida signa señales moduladas de cada frecuencia portadora y las pasa al canal de salida apropiado, al cual el teléfono del abonado está conectado directamente.

Los switches FDM pueden llevar a cabo tanto la conmutación dinámica como la permanente. Cuando se utiliza la conmutación dinámica, un abonado inicia una conexión con otro mediante el envío del número telefónico del abonado que es llamado a través de la red. El switch asigna de manera dinámica a ese abonado una de las bandas disponibles del canal multiplexado. Cuando se utiliza la conmutación permanente, la banda de 4 KHz se asigna al abonado por un tiempo prolongado sintonizando el switch a una entrada específica, la cual no está disponible para los demás abonados.

El principio de la conmutación FDM no varía en otro tipo de redes, sino sólo cambian los límites de las bandas asignadas a loops locales específicos, así como varios canales de baja velocidad dentro de un solo canal de alta velocidad.

El **método WDM** aplica el mismo principio de FDM en otra área del espectro electromagnético. La señal de información aquí no es una corriente eléctrica ni una onda de radio, sino que es la luz. Para organizar los canales WDM en la fibra óptica, se usan las ondas de las tres ventanas de transmisión, las cuales corresponden al rango del infrarrojo, que tiene una longitud de onda en el rango de 850 nm a 1 565 nm o a frecuencias que van de 196 a 350 THz.

En el enlace troncal, varios canales espectrales se multiplexan generalmente: 16, 32, 40, 80 o 160 (comenzando desde 16 canales). Esta técnica de multiplexaje se llama **WDM denso** (**DWDM**). Dentro de dichos canales espectrales, los datos pueden codificarse mediante una técnica analógica o una discreta. Las técnicas WDM y DWDM son implementaciones de la idea del multiplexaje de frecuencia analógica, pero en forma diferente. La diferencia entre las redes WDM o DWDM y las FDM reside en su máxima velocidad de transmisión de información. Las redes FDM por lo general garantizan la transmisión simultánea de hasta 600 conversaciones utilizando la troncal, la cual corresponde a una velocidad total de 36 Mbps. En comparación, en los canales digitales, la velocidad se recalcula con base en la asignación

de 64 Kbps por conversación, y las redes DWDM por lo regular garantizan una utilización total de cientos de gigabits o aun terabits por segundo.

La tecnología DWDM se estudiará con más detalle en el capítulo 11.

9.6.2 Conmutación de circuitos basada en TDM

La técnica de conmutación de circuitos basada en FDM fue diseñada para transmitir señales analógicas que representan voz. Cuando se migró a la forma digital para representar la voz, se ideó una nueva técnica de multiplexaje orientada hacia la naturaleza discreta de los datos transmitidos.

Dicha técnica se conoce como *TDM*. El principio de TDM consiste en asignar un canal a cada conexión por un tiempo específico. Se utilizan dos tipos de TDM: asincrónico y sincrónico. El lector ya conoce el **modo TDM asincrónico**, pues se utiliza en las redes de conmutación de paquetes. Cada paquete usa el canal por el tiempo específico que se requiere para transmitirlo entre los puntos terminales del canal. No existe ninguna sincronía entre los diferentes flujos de información y cada usuario intenta usar el canal cuando es necesario transmitir información.

En esta sección se describirá el **modo TDM sincrónico**,[4] en el que todos los flujos de información tienen un acceso sincronizado al canal. Como resultado, cada flujo de información periódicamente tiene el canal a su disposición por un tiempo fijo llamado **ranura de tiempo**.

La figura 9.12 muestra el principio de la conmutación de circuitos basada en el método TDM para el ejemplo de la transmisión de voz.

El equipo de las redes TDM —multiplexores, switches y demultiplexores— opera en el modo de tiempo compartido, sirviendo a todos los canales por turnos durante el ciclo de operación. El ciclo de operación del equipo TDM es igual a 125 μseg, el cual corresponde al periodo entre mediciones consecutivas de voz en el canal digital. Esto significa que el multiplexor o switch cuenta con tiempo para servir a cualquier canal y transmitir las mediciones consecutivas más lejos mediante el uso de la red. A cada conexión se le asigna un espacio de tiempo del ciclo de operación del equipo, conocida como *ranura de tiempo*, como se mencionó con antelación. La longitud de la ranura de tiempo depende del número de canales servidos por el multiplexor TDM o switch.

El *multiplexor* recibe información a través de N canales de entrada, cada uno de los cuales transmite datos a una velocidad de 64 Kbps (es decir, 1 byte cada 125 μseg). Durante cada ciclo, el multiplexor lleva a cabo las operaciones siguientes:

- Recibe el siguiente byte de datos de cada canal.
- Genera una trama con los bytes recibidos.
- Transmite la trama multiplexada hacia el canal de salida a una velocidad igual a $N \times 64$ Kbps.

El orden de los bytes en la trama multiplexada corresponde al número del canal de entrada del que se recibió el byte. El número de canales atendidos por el multiplexor depende de su velocidad de operación. Por ejemplo, el multiplexor T1, que fue el primer multiplexor industrial que operó con base en la tecnología TDM, soporta 24 canales de entrada y genera

[4] Es necesario mencionar que cuando se utiliza la abreviatura TDM sin especificar el modo de operación, siempre significa modo TDM sincrónico.

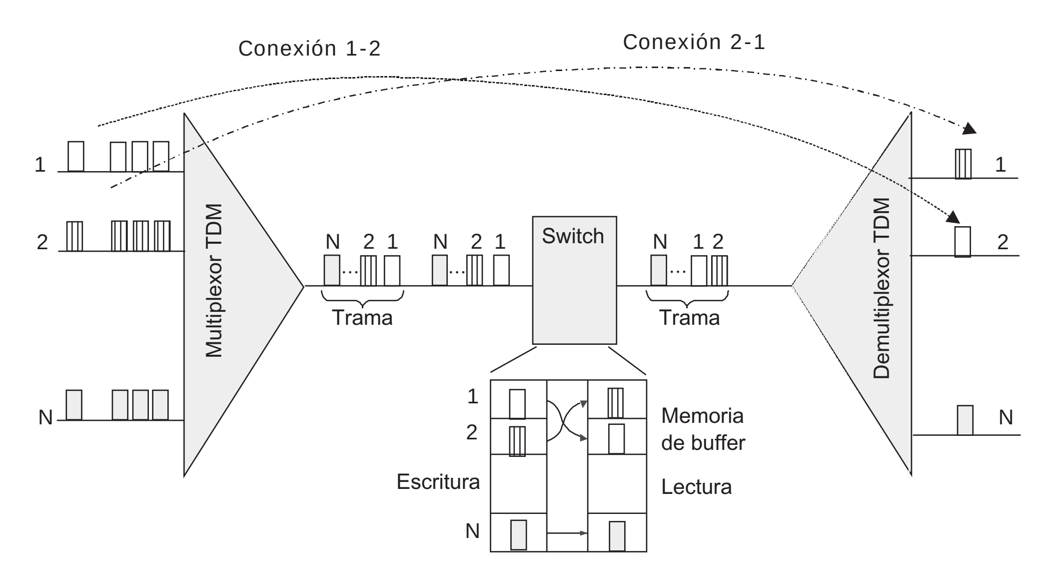


FIGURA 9.12 Conmutación de circuitos basada en TDM.

a la salida *tramas fundamentales estándar T1* que se transmiten a una velocidad de 1 544 Mbps.

El *demultiplexor* lleva a cabo la función inversa: analiza los bytes que conforman la trama y las distribuye a través de sus canales de salida, al considerar que el número ordinal de bytes en la trama fundamental corresponde al número del canal de salida.

El *switch* recibe la trama a través de un canal de alta velocidad del multiplexor y escribe cada byte de esta trama en una celda independiente de su memoria buffer en el mismo orden en el que los bytes fueron empacados en la trama multiplexada. Para llevar a cabo la conmutación, los bytes son recuperados de la memoria buffer en el orden correspondiente al número de abonado conectado por el canal específico y no en el orden de su llegada. Por ejemplo, si el primer abonado en la parte izquierda de la red (figura 9.12) se conecta al segundo abonado en la parte derecha de la red, el byte escrito en la primera celda de la memoria buffer será el segundo byte recuperado. Si se mezclan los bytes dentro de la trama en el orden deseado, el switch asegurará el establecimiento de las conexiones entre abonados.

El número asignado de la ranura de tiempo está a disposición de la conexión entre el canal de entrada y la ranura de salida durante toda la conexión, aun si el tráfico se transmita en ráfagas y no siempre requiera usar el número de ranuras de tiempo asignadas. Esto significa que una conexión en una red TDM siempre tiene un ancho de banda constante y conocido, el cual es un múltiplo de 64 Kbps.

La operación del equipo TDM es similar a la de las redes de conmutación de paquetes, ya que cada byte puede considerarse un paquete elemental. Sin embargo, en contraste con el paquete de una red de computadoras, el paquete en una red TDM no tiene una dirección individual. El papel de su dirección se delega al número ordinal de bytes dentro de la trama fundamental o el número de su ranura de tiempo asignada en el multiplexor o switch. Las redes que utilizan la técnica TDM requieren la operación sincrónica de todo el equipo, debido a lo cual el segundo nombre de esta tecnología es **modo de transferencia sincrónica** o **STM.**

La violación a la sincronía incumple con el requerimiento de conmutación entre abonados, ya que la información acerca de la dirección se pierde. Por lo tanto, la redistribución dinámica de ranuras de tiempo entre los diferentes canales en el equipo TDM es imposible

aun si, en un ciclo específico de la operación del multiplexor, la ranura de tiempo en un canal determinado demuestra ser redundante debido a que no hay datos por transmitir a la entrada de ese canal. Un ejemplo es un abonado telefónico que está en silencio.

Existe una modificación de la técnica TDM, conocida como **TDM estadístico** (**STDM**), la cual fue diseñada específicamente para dar la posibilidad de aumentar el ancho de banda de otros canales en el caso de que las ranuras de tiempo de algunos canales estén disponibles temporalmente. Para llevar a cabo esta tarea, cada byte se complementa con el campo corto de direcciones (por ejemplo, 4 o 5 bits), el cual permite el multiplexaje de 16 o 32 canales. STDM es la técnica de conmutación de paquetes que tiene direccionamiento simplificado y un área de aplicación limitada, por ello se utiliza principalmente con equipo no estándar para conectar terminales a equipos grandes. La tecnología del **modo de transferencia asincrónica** (**ATM**) es un desarrollo más allá de las ideas del multiplexaje estadístico. ATM es una técnica de conmutación de paquetes.

Las redes TDM pueden soportar el modo de conmutación dinámica, el modo de conmutación permanente o ambos. Por ejemplo, el modo principal de las redes telefónicas digitales que operan con base en la tecnología TDM es la conmutación dinámica. No obstante, dichas redes también soportan la conmutación permanente y proporcionan a sus suscriptores servicios de líneas arrendadas.

9.6.3 Modo dúplex de operación de canales

El modo dúplex es la manera más universal y eficaz de operación de un canal. La variante más simple de garantizar el modo dúplex consiste en usar dos enlaces físicos independientes (por ejemplo, dos pares de alambres o dos fibras ópticas) en el cable, cada uno de los cuales opera en el modo símplex (es decir, transmite datos en una sola dirección). Esta idea sirvió como base en la implementación de muchas tecnologías de red, entre ellas Fast Ethernet y ATM.

A veces, dichas soluciones simples muestran ser ineficaces o imposibles. Con mucha frecuencia, esto sucede cuando sólo un enlace físico se encuentra disponible para el intercambio de datos en forma dúplex y la organización de un segundo enlace requiere una inversión significativa. Por ejemplo, cuando se intercambian datos a través de redes telefónicas mediante módems, los usuarios solamente cuentan con un enlace físico que se conecta a la central automática —un par de líneas—. Desde el punto de vista económico es ineficaz comprar otra. En dichos casos, el modo dúplex está organizado con base en la división del canal en dos canales lógicos utilizando técnicas FDM o TDM.

Cuando se usa FDM para organizar un canal dúplex, la banda de frecuencias se divide en dos partes. Esta división puede ser simétrica o asimétrica. En el último caso, las velocidades de transmisión de información en cada sentido son diferentes. Un ejemplo muy común de la forma en la que se realiza este método es la tecnología ADSL utilizada para el acceso a Internet de banda ancha. Cuando FDM garantiza el modo de operación dúplex recibe el nombre de **dúplex por división de frecuencia** (**FDD**).

Cuando se usa la codificación digital, el modo dúplex en una línea de dos alambres está organizado al aplicar la técnica TDM. Parte de la ranura de tiempo se emplea para transmitir datos en una dirección; la otra parte es para llevar datos en la otra dirección. En general, las ranuras de tiempo en direcciones opuestas están mezcladas; por lo tanto, dicho método a veces se llama *transmisión ping-pong*. El modo TDM dúplex se conoce con el nombre de **dúplex por división de tiempo** (**TDD**).

En los cables de fibra óptica con una sola fibra se puede aplicar la tecnología DWDM a la implementación del modo de operación dúplex. La transmisión de datos en una direc-

ción se lleva a cabo mediante la aplicación de un rayo de luz con una longitud de onda, y la transmisión de datos en la dirección opuesta se lleva a cabo con el empleo de un rayo de luz a otra longitud de onda. De hecho, la solución a este problema en particular —organizar dos canales espectrales diferentes dentro de una sola ventana de transmisión— dio como resultado el desarrollo de la tecnología WDM, la cual se convirtió en DWDM.

El advenimiento de *procesadores de señales digitales (DSP)* de gran poder capaces de llevar a cabo algoritmos sofisticados para el procesamiento de señales en tiempo real facilitó implementar otra variante del modo dúplex. En este caso, dos transmisores operan de manera simultánea en direcciones opuestas creando la señal aditiva total en el canal. Como cada transmisor conoce el espectro de su señal, lo resta de la señal total y, como resultado de este proceso, recibe la señal enviada por el otro transmisor.

RESUMEN

- Para representar información discreta, se utilizan dos tipos de señales: pulsos rectangulares y ondas senoidales. En el primer caso, el método de representación se llama *codificación* y en el segundo *modulación*.
- Cuando se transmite información discreta, los unos y los ceros se codifican mediante cambios en la amplitud, frecuencia o fase de la señal senoidal.
- Para aumentar la velocidad de datos, se usan métodos combinados de modulación. El método más utilizado es el de *modulación de amplitud en cuadratura*. Dichos métodos se basan en la combinación de la modulación en amplitud y en fase.
- Cuando se selecciona el método de codificación, es necesario alcanzar varias metas de manera simultánea:
  - Minimizar el ancho posible del espectro de la señal resultante.
  - Garantizar la sincronización entre el transmisor y el receptor.
  - Garantizar la resistencia al ruido.
  - Detectar y, de ser posible, corregir errores.
  - Minimizar la potencia del transmisor.
- El espectro de la señal es una de las características más importantes del método de codificación. El espectro angosto de las señales permite lograr una velocidad de transmisión de datos mayor, al contar con un ancho de banda constante del medio de transmisión.
- El código debe brindar propiedades de autosincronización, lo cual significa que sus señales deben contener indicaciones de acuerdo con las cuales el receptor pueda determinar en qué instancia en el tiempo es necesario llevar a cabo el reconocimiento del siguiente bit.
- Cuando se utiliza la codificación discreta, la información binaria se representa mediante diversos niveles de voltaje constante o por medio de la polaridad del pulso.
- El código de no retorno a cero (NRZ) es el código potencial más simple, pero no ofrece facilidades para la autosincronización.
- Con la finalidad de mejorar las propiedades del código potencial NRZ, se utilizan métodos especiales que implementan la sincronización. Dichos métodos se basan en lo siguiente:
  - La introducción de bits redundantes en los datos de la fuente.
  - Aleatorización de los datos de la fuente.

- Los códigos Hamming y los de convolución no solamente permiten detectar errores repetitivos, sino también corregirlos. Dichos códigos se utilizan con mucha frecuencia como herramientas para la corrección de errores hacia delante.
- Para mejorar las velocidades efectivas de transmisión de datos en las redes, se utiliza la condensación de datos dinámica basada en diferentes algoritmos. La relación de condensación depende del tipo de datos y del algoritmo utilizado y puede variar dentro del rango de 1:2 a 1:8.
- Para organizar varios canales dentro de un enlace de transmisión, se emplean varios métodos de multiplexaje: por división de frecuencia, por división de tiempo (TDM), por división de longitud de onda y el acceso múltiple por división de código. Las técnicas de conmutación de paquetes son compatibles solamente con TDM; sin embargo, las técnicas de conmutación de circuitos pueden usar cualquier otro tipo de multiplexaje.

PREGUNTAS DE REPASO

1. ¿Cuáles son las ventajas y las desventajas del código NRZ?
2. ¿Qué tipo de información se transmite mediante el uso de ASK?
3. ¿Por qué la modulación ASK no se utiliza con canales de banda ancha?
4. ¿Qué parámetros de la senoidal cambian cuando se emplea el método QAM?
5. ¿Cuántos bits se transmiten por carácter en un código que tiene siete estados?
6. Explique las razones por las que el ancho de banda de 64 Kbps se ha seleccionado para representar el canal elemental de las redes telefónicas.
7. ¿Qué método se utiliza para mejorar las propiedades de autosincronización del código B8ZS?
8. ¿Cuáles son las diferencias entre la codificación lógica y la física?
9. ¿Qué principios sirven como base para aplicar los métodos de detección y corrección de errores?
10. Haga una lista de los métodos de condensación más apropiados para la información textual. ¿Por qué son ineficaces para condensar datos binarios?
11. ¿Qué es la distancia de Hamming?
12. ¿Cuál es el valor de la distancia de Hamming en los métodos de control de paridad?
13. ¿Es posible utilizar el multiplexaje por división de frecuencia en una red Ethernet?
14. ¿Qué modo TDM se usa en las redes de conmutación de paquetes?
15. ¿Es posible combinar diferentes métodos de multiplexaje? En caso afirmativo, proporcione algunos ejemplos.
16. ¿Cuáles son las características comunes de los métodos FDM y WDM?
17. ¿Con base en cuál técnica se implementa el modo dúplex en un canal si ambos transmisores utilizan el mismo rango de frecuencia en forma simultánea?

PROBLEMAS

1. Encuentre las primeras dos armónicas del espectro de la señal NRZ cuando se transmite la secuencia 110011001100… si la frecuencia del transmisor es de 100 MHz.
2. ¿Cuál de los 16 códigos seleccionaría usted para transmitir información del usuario cuando usara el código 3B/4B?
3. Sugiera un código redundante con una distancia de Hamming de 3 bits.

4. ¿Es posible transmitir confiablemente los datos a través de un canal con un ancho de banda de 2.1 GHz a 2.101 GHz si se utilizan los siguientes parámetros de transmisión: frecuencia de la portadora de 2.1005 GHz, modulación ASK con dos valores de amplitud y una frecuencia de reloj de 5 MHz?
5. Sugiera códigos de longitud variable para cada uno de los caracteres A, B, C, D, F y O si fuera necesario transmitir el mensaje siguiente: BDDACAAFOOOAOOOO. ¿Es posible lograr una condensación comparable con las del uso de:
   - Códigos ASCII convencionales?
   - Códigos con longitud fija tomando en cuenta sólo la presencia de los caracteres listados anteriormente?
6. ¿Cuántas veces mejoraría el ancho espectral de la señal NRZ si la frecuencia de reloj del transmisor se duplicara?

10

TRANSMISIÓN INALÁMBRICA

DESCRIPCIÓN DEL CAPÍTULO

10.1 INTRODUCCIÓN

La transmisión inalámbrica se popularizó como medio de comunicación tan sólo unos cuantos años después de la transmisión a través de medios guiados. En la década de 1890 ya se habían llevado a cabo los primeros experimentos en el campo de la transmisión de mensajes telegráficos a través de señales de radio, mientras que en el decenio de 1920 la gente comenzó a utilizar la radio para la transmisión de voz.

En la actualidad, existen varios sistemas de comunicaciones inalámbricas, los cuales no están limitados a la difusión vasta como la televisión y la radio. Los sistemas inalámbricos se usan ampliamente como medio de transporte para la transmisión de información discreta. Para construir enlaces de comunicaciones de larga distancia están disponibles los sistemas de radio y los satelitales. Los sistemas de acceso inalámbrico sirven también para tener acceso a las redes de comunicaciones de larga distancia y para las LAN inalámbricas.

El medio de transmisión inalámbrico utiliza principalmente el rango de las microondas y se caracteriza por poseer altos niveles de ruido, el cual es generado por fuentes externas de radiación, así como por las múltiples reflexiones de señales en paredes y otro tipo de barreras. Por lo tanto, los sistemas de comunicaciones inalámbricos tienen que implementar varios métodos para suprimir el ruido. Entre la gama de dichas herramientas se encuentran los códigos de corrección de errores hacia delante, los cuales se estudiarán en líneas ulteriores, así como los protocolos con reconocimiento de entrega de la información. Una técnica diseñada especialmente para los sistemas inalámbricos, llamada *técnica de espectro disperso*, representa una herramienta eficaz para la supresión del ruido.

En este capítulo se proporcionará la información básica acerca de los elementos, principios de operación y métodos de codificación de los sistemas inalámbricos que se utilizan para construir canales de comunicación punto a punto, punto a multipunto y multipunto a multipunto.

10.2 MEDIOS DE TRANSMISIÓN INALÁMBRICOS

PALABRAS CLAVE: IEEE 802.11, comunicaciones inalámbricas móviles, comunicaciones inalámbricas fijas, telefonía móvil, red móvil, enlace inalámbrico, propagación direccional y omnidireccional de ondas, antena parabólica, antena isotrópica, espectro electromagnético, banda de radio, banda de microondas, banda del infrarrojo, loops locales inalámbricos (WLL), reflexión, difracción, dispersión, propagación multitrayectoria, interferencia intersimbólica, desvanecimiento multitrayectoria, legislación, licitación comparativa, subasta y rangos industrial, científico y médico (ISM).

10.2.1 Ventajas de las comunicaciones inalámbricas

La posibilidad de transmitir información sin cables y, por lo tanto, de liberar a los usuarios de la necesidad de estar limitados a un espacio específico siempre ha representado un atractivo especial. Siempre que esté disponible la tecnología suficiente para garantizar que el nuevo servicio inalámbrico tenga los dos componentes requeridos para funcionar de manera adecuada, conveniencia de uso y bajo costo, su éxito estará prácticamente garantizado.

La telefonía móvil se convirtió en la prueba más reciente de esto. El primer teléfono móvil fue inventado por *Lars Magnus Ericsson* en 1910 para ser usado en automóviles, pero sólo era inalámbrico de camino. En estas condiciones, era imposible utilizar el dispositivo. Para



FIGURA 10.1 Primer teléfono de automóvil (publicado con el permiso del autor: Anders Suneson).

hacer una llamada, el conductor tenía que detener el auto; luego utilizaba un par de garruchas de considerable longitud con el fin de conectar el teléfono a los alambres telefónicos que existían en postes al lado de la carretera (figura 10.1). Como era natural, la inconveniencia de su uso, así como su limitada movilidad, evitaron que este tipo de teléfono fuera un éxito comercial.

Transcurrió un largo tiempo antes de que las tecnologías de acceso por radio fueran bastante maduras para garantizar la producción de radioteléfonos en apariencia compactos y con bajo costo. A finales de la década de 1970 comenzó el uso masivo de la telefonía móvil que continúa hasta hoy en día.

Las comunicaciones inalámbricas no implican sólo las comunicaciones inalámbricas móviles. También existen **comunicaciones inalámbricas fijas** en las que los nodos por comunicar están ubicados dentro de los límites de una pequeña área, por ejemplo: un edificio, un territorio o un distrito.

Si por alguna razón el uso de un sistema de cableado es imposible o resulta ineficaz, se utilizan las comunicaciones inalámbricas fijas en lugar de aquellas con un medio de transmisión guiado. Las razones para ello pueden diferir ampliamente. Las áreas poco pobladas y los lugares de difícil acceso (como regiones cenagosas, la selva en Brasil, los desiertos, y las regiones árticas y antárticas) tendrían que esperar un largo tiempo para tener su sistema de cableado. Los edificios que son monumentos históricos y en cuyas paredes no pueden instalarse cables representan otro ejemplo. Otra situación muy común es aquella en la que debe brindarse acceso a usuarios cuyas casas se encuentran conectadas a puntos de presencia de portadores que ya se encontraban posicionados. Por último, a veces se requiere instalar sistemas de comunicaciones de manera temporal. Considérese, por ejemplo, una conferencia que se va a llevar a cabo en un edificio que no cuenta con enlaces de cable capaces de garantizar una velocidad de comunicación suficiente para brindar un servicio de alta calidad a todos los participantes.

Las comunicaciones inalámbricas se han utilizado para la transmisión de datos por mucho tiempo. Hasta fechas recientes, la mayoría de sus aplicaciones en las redes de computadoras estaban limitadas a una variante fija. Los usuarios de las redes y aun sus arquitectos no siempre están conscientes de que en ciertos fragmentos de la trayectoria de la red, la información no es transmitida por medio de alambres. En lugar de eso, se propaga a través de la atmósfera o espacio terrestre en forma de ondas electromagnéticas. Esto puede suceder cuando una computadora arrienda un canal de un prestador de servicios de comunicaciones y el enlace específico de dicho canal es un enlace satelital o de microondas terrestres.

A mediados de la década de 1990, la **tecnología de las redes móviles** alcanzó un alto nivel de madurez. Con la adopción del estándar IEEE 802.11 en 1997, fue posible construir las redes Ethernet móviles, las cuales garantizaban la comunicación entre usuarios sin importar su ubicación ni el fabricante o proveedor del equipo que utilizaban. Por el momento, dichas redes desempeñan un papel muy modesto comparado con las redes de telefonía móviles. Sin embargo, la mayoría de los analistas predice un gran crecimiento en esta área en un futuro cercano.

Con mucha frecuencia, las redes inalámbricas están asociadas con las *señales de radio,* aunque esto no siempre es correcto. Las comunicaciones inalámbricas usan un amplio rango del espectro electromagnético, que varía desde las ondas de radio de baja frecuencia (varios Hertz) hasta la luz visible (alrededor de 8×10^{14} Hz).

10.2.2 Enlace inalámbrico

Un *enlace inalámbrico* se construye de acuerdo con un método muy simple (figura 10.2).

Cada nodo está equipado con una antena, la cual funciona simultáneamente como transmisor y receptor de ondas electromagnéticas. Dichas ondas se propagan a través de la atmósfera o en el vacío a una velocidad de 3×10^8 m/seg.

Las ondas electromagnéticas pueden propagarse en todas direcciones (*omnidireccionales*) o dentro de un sector específico (*direccional*). El tipo de propagación depende de la clase de antena. La figura 10.2 muestra una **antena parabólica** direccional.

Una **antena isotrópica** también es una antena muy común: consiste en un conductor vertical con una longitud igual a un cuarto de la longitud de onda de radiación. Dichas antenas son *omnidireccionales* y se utilizan mucho en automóviles y dispositivos portátiles. La propagación omnidireccional de las ondas electromagnéticas también puede garantizarse mediante el uso de varias antenas direccionales.

En la propagación omnidireccional, las ondas electromagnéticas llenan todo el espacio dentro de los límites de cierto radio determinado por la atenuación de la potencia de la señal. Dicho espacio se convierte en un medio de transmisión compartido. Al compartirse el medio de transmisión surgen los mismos problemas que con las LAN; sin embargo, en las comunicaciones inalámbricas, la situación empeora debido a que el espacio en los alrededores está abierto para el acceso del público. Esto contrasta con los cables, los cuales pertenecen a organizaciones específicas.

Un medio de transmisión inalámbrico a menudo recibe el nombre de no guiado, en contraste con el medio guiado, donde el conductor (alambre de cobre o fibra óptica) define estrictamente la dirección de propagación de la señal.

Para transmitir información discreta utilizando un canal inalámbrico, es necesario modular oscilaciones electromagnéticas del transmisor empleando el flujo de bits que se

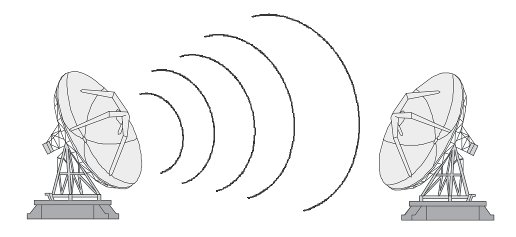


FIGURA 10.2 Enlace de transmisión inalámbrico.

transmiten. Esta función es realizada por el dispositivo DCE que conecta a la computadora, al switch o al ruteador de la red de computadoras y la antena.

10.2.3 Espectro electromagnético

Las características de los enlaces de comunicaciones inalámbricos —la distancia entre nodos, el territorio cubierto, la velocidad de transmisión de la información, etc.— en muchos sentidos dependen de la frecuencia del espectro electromagnético que se utilice. La frecuencia f y la longitud de onda λ están relacionadas mediante la fórmula siguiente:

$$c = f \times \lambda \tag{10.1}$$

La figura 10.3 muestra las bandas de frecuencia del espectro electromagnético. Cuando éstas se estudian, es posible decir que los sistemas de comunicaciones inalámbricas se encuentran en uno de los cuatro grupos siguientes:

La banda que va de los 20 a los 300 GHz se llama **banda de radio**. La ITU la ha dividido en varios subrangos (la fila inferior de flechas en la figura 10.3) que van desde la *extremadamente baja frecuencia* (ELF) hasta la *extremadamente alta frecuencia* (EHF). Las estaciones de radio a las que estamos acostumbrados con las que la radio suele asociarse trabajan en el rango de 20 KHz a 300 MHz. Para estos rangos, se usa mucho un nombre especial a pesar de no estar definido en los estándares: *difusión por radio*. Este grupo incluye los sistemas de baja velocidad que utilizan los rangos de la modulación de amplitud (AM) y la modulación de frecuencia (FM) para transmitir datos a velocidades que van de las decenas hasta los cientos de kilobits por segundos. Ejemplos de dichos dispositivos son los radio módems que conectan dos segmentos de la misma LAN a velocidades de 2 400, 9 600 o 19 200 Kbps.

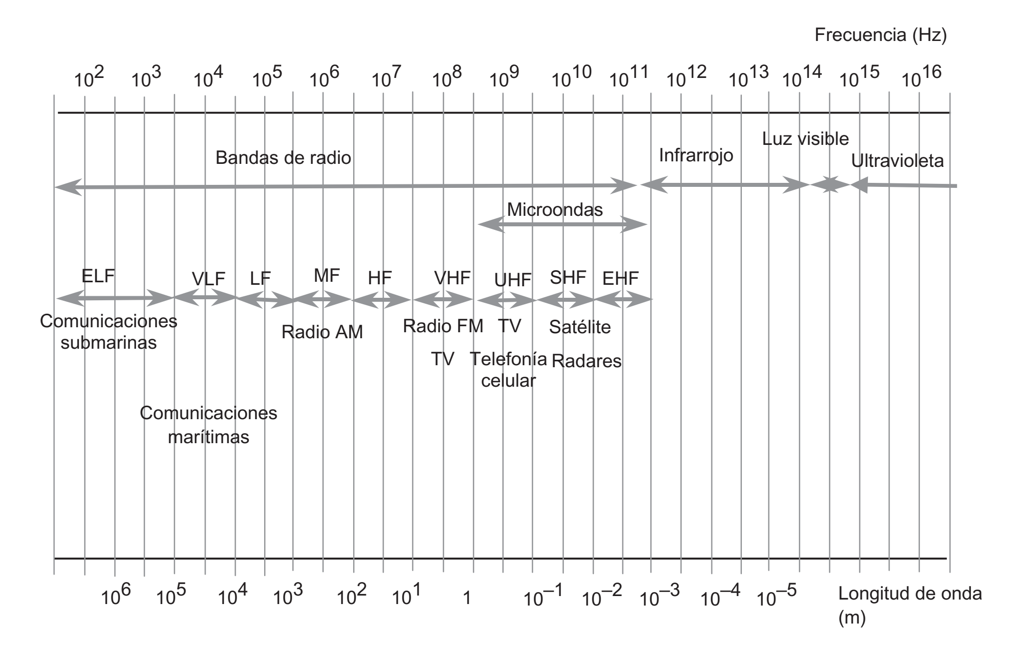


FIGURA 10.3 Bandas de frecuencia del espectro electromagnético.

El rango de 300 MHz a 3 000 GHz también tiene un nombre no estandarizado: **banda de microondas**, que constituye la clase más amplia de sistemas que abarcan las líneas de radio, los canales satelitales, las LAN inalámbricas y las redes de acceso inalámbrico fijo. También se les conoce con el nombre de *loops locales inalámbricos (WLL)*.

Exactamente arriba de la banda de microondas está la **banda del infrarrojo**. Las bandas de las microondas y del infrarrojo se utilizan mucho también para la transmisión de información de manera inalámbrica. Como este tipo de radiación no puede penetrar las paredes, los sistemas de este tipo se utilizan para construir pequeños segmentos LAN dentro de una sola habitación.

Banda de luz visible. En años pasados, la luz visible también ha encontrado aplicaciones en la transmisión de información utilizando láseres. Dichos sistemas se usan como una alternativa de alta velocidad en canales inalámbricos punto a punto para organizar el acceso en cortas distancias.

NOTA *La luz visible fue probablemente el primer medio de transmisión utilizado para las comunicaciones inalámbricas, ya que se empleó en las civilizaciones muy antiguas (por ejemplo, en Grecia) para la transmisión de señales a lo largo de cadenas de observadores situados en las cimas de las montañas.*

10.2.4 Propagación de ondas electromagnéticas

Existen algunos patrones comunes de propagación de ondas electromagnéticas relacionadas con la frecuencia de radiación:

Conforme la frecuencia de la portadora sea más alta, es posible alcanzar velocidades más elevadas de transmisión de información.

A medida que la frecuencia es más elevada, las características de penetración de la señal a través de paredes y otras barreras serán más pobres. Las ondas de radio de baja frecuencia de las bandas de AM penetran fácilmente las casas, permitiendo así a los usuarios domésticos recibir con una antena casera. Las señales de televisión, las cuales tienen frecuencias mayores, generalmente requieren una antena externa. Por último, la radiación infrarroja y la luz visible no pueden penetrar paredes, limitando así la transmisión a través de línea de vista.

A medida que la frecuencia es mayor, la energía de la señal se disminuirá más rápido con el aumento de la distancia respecto al transmisor. Cuando las ondas electromagnéticas se propagan a través del espacio libre (sin reflexiones), la atenuación de la potencia de la señal es proporcional al producto del cuadrado de la distancia respecto a la fuente y el cuadrado de la frecuencia de la señal.

Las señales con frecuencias bajas, hasta los 2 MHz, se propagan a lo largo de la superficie terrestre. Por esta razón, las señales de radio de AM pueden propagarse a distancias de cientos de kilómetros.

Las señales con frecuencias que varían de 2 a 30 MHz se reflejan en la ionosfera de la Tierra. En consecuencia, éstas pueden propagarse a distancias aún mayores: miles de kilómetros si el transmisor es lo suficientemente potente.

Las señales que varían en el rango superior a 30 MHz se propagan en línea recta solamente, lo cual significa que son señales de línea de vista. A frecuencias mayores a los 4 GHz, se presentan algunos problemas. Por ejemplo, las señales pueden ser absorbidas por el agua, lo cual significa que no sólo la lluvia sino también la niebla pueden degradar significativamente la calidad de la transmisión de los sistemas de microondas. Ésa es una razón por la que las pruebas de los sistemas de transmisión de datos basados en láser a menudo se llevan a cabo en Seattle, una ciudad famosa por sus frecuentes lluvias.

La necesidad de contar con una rápida transmisión de datos es enorme; por lo tanto, todos los sistemas de comunicaciones inalámbricos actuales operan en las bandas de alta frecuencia, comenzando en los 800 MHz, a pesar de las ventajas de la propagación de la señal a lo largo de la superficie terrestre o su reflexión en la ionosfera, las cuales son proporcionadas por las bandas de baja frecuencia.

Para optimizar el uso del rango de microondas, también es necesario tomar en cuenta los problemas adicionales encontrados por las señales que se propagan en modo línea de vista y que se encuentran con obstáculos a lo largo de su camino.

La figura 10.4 muestra que una señal que encuentra un obstáculo puede propagarse de acuerdo con los tres mecanismos siguientes: reflexión, difracción y dispersión.

Cuando la señal se topa con un obstáculo, el cual es parcialmente transparente para la longitud de onda de la señal y es de un tamaño que excede de modo significativo la longitud de onda de la señal, parte de su energía se **refleja** de tal modo que se aleja del obstáculo. Las ondas de las bandas de microondas tienen longitudes de onda de varios centímetros. Por lo tanto, éstas son reflejadas de manera parcial en las paredes de los edificios cuando la transmisión de las señales se lleva a cabo en una ciudad.

Si la señal se topa con una barrera impenetrable (por ejemplo, una placa de metal) cuyo tamaño excede significativamente a la longitud de onda de la señal, se presentará el fenómeno de la **difracción**. En este caso, la señal rodea el obstáculo de modo tal que es posible recibir la señal, a pesar de que no está dentro de la zona de línea de vista.

Por último, cuando una señal se topa con una barrera cuyo tamaño es comparable con la longitud de onda, ésta se **dispersa** y comienza a propagarse con ángulos diferentes.

Debido a estos mecanismos, que son comunes en las comunicaciones inalámbricas dentro de las ciudades, pueden llegar varias copias de la misma señal al receptor. Dicho efecto se conoce con el nombre de **propagación multitrayectoria**. Los resultados de la propagación multitrayectoria son, con mucha frecuencia, negativos debido a que una de las copias puede llegar fuera de fase, eliminando a la señal principal. Por lo general, el tiempo de propagación a lo largo de trayectorias distintas es diferente. También puede ocurrir un efecto conocido como **interferencia intersimbólica**, que corresponde a situaciones en las que los retardos provocan que las señales que codifican a los bits de datos adyacentes lleguen al receptor de manera simultánea. Las distorsiones provocadas por la propagación multitrayectoria resultan en una atenuación de la señal, un efecto conocido como **desvanecimiento por multitrayectoria**. En las ciudades, el desvanecimiento multitrayectoria da como resultado una atenuación de la señal proporcional a la tercera o aun a la cuarta potencia de la distancia, en lugar de al cuadrado de la misma.

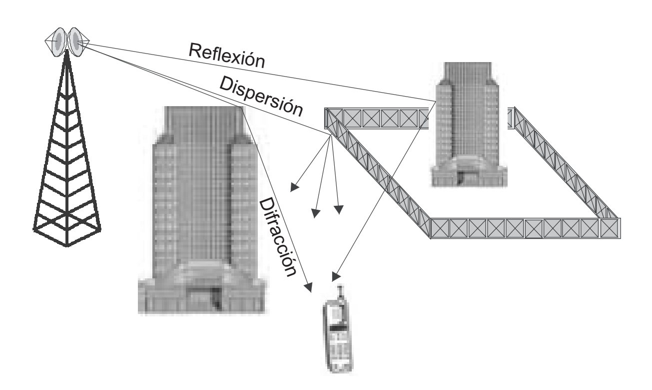


FIGURA 10.4 Propagación de ondas electromagnéticas.

Todas estas distorsiones que experimenta la señal, que son numerosas y poderosas en las ciudades, se combinan con el ruido electromagnético externo. Es suficiente mencionar que los hornos de microondas también trabajan en la banda de 2.4 GHz.

NOTA *La movilidad que se gana por medio de la ausencia de cables tiene un costo. En este caso, dicho precio es el alto nivel de ruido en los canales de comunicación inalámbrica. Éste es un problema común en todos los tipos de comunicaciones inalámbricas. En las bandas de alta frecuencia de mayor interés, este problema se convierte en algo muy serio. En contraste con la probabilidad de errores de bits en los enlaces de comunicaciones guiados (10^{-9} o 10^{-10}), en los enlaces de comunicaciones alámbricos, ¡llega a tener un valor de 10^{-3}!*

El problema de los altos niveles de ruido en los enlaces inalámbricos puede resolverse si se utilizan varios métodos. Los métodos de codificación especial que distribuyen la energía de la señal en un rango amplio de frecuencias desempeñan un papel muy importante; además, es una práctica muy común instalar transmisores de señales (y, si es posible, receptores) en torres elevadas con el fin de evitar posibles reflexiones.

El uso de protocolos orientados a la conexión que garantizan la retransmisión de tramas a nivel capa de enlace de datos de la pila de protocolos representa otro método muy utilizado. Este método permite corregir errores más rápido, ya que los protocolos de transporte como el TCP trabajan con tiempos de espera prolongados.

10.2.5 Legislación

Las ondas electromagnéticas se pueden propagar en todas direcciones a través de grandes distancias y son capaces de penetrar barreras tales como paredes. Por lo tanto, el problema de compartir bandas del espectro electromagnético es urgente y requiere un control centralizado. Cada país cuenta con una autoridad especializada que, de acuerdo con las recomendaciones del ITU, otorga **licencias** a los prestadores de servicios de comunicaciones, permitiéndoles usar una banda específica del espectro suficiente para transmitir información según la tecnología seleccionada. La licencia es otorgada a un territorio específico dentro del cual el prestador de servicios tiene los derechos exclusivos de utilizar la banda de frecuencias asignada.

Para el otorgamiento de frecuencias, las autoridades gubernamentales utilizan varias estrategias. Las más populares se listan en seguida:

Licitación comparativa. Los prestadores de servicios que participan en la licitación comparativa desarrollan ofrecimientos detallados. En estos documentos, describen sus servicios planeados, las tecnologías que utilizarán para implementar dichos servicios, los niveles de precios para clientes potenciales, etc. Después, el comité analiza todas las ofertas y selecciona a la compañía que mejor satisfaga las necesidades y expectativas de la comunidad. La complejidad de los criterios utilizados en la selección del ganador a menudo resulta en retrasos significativos del proceso de la toma de decisiones e incluso en corrupción entre los oficiales. Por esta razón, algunos países, incluido Estados Unidos, ya no usan este método. No obstante, en otros países todavía se utiliza con mucha frecuencia cuando se toman decisiones relacionadas con los servicios vitales para dichos países, como el uso de los sistemas 3G.

Lotería. La lotería constituye el método más justo y rápido, pero no siempre produce los mejores resultados. Esto sucede especialmente cuando participan falsos prestadores de servicios en la lotería (es decir, aquellos que planean revender la licencia en vez de prestar los servicios por sí mismos).

Subasta. Las subastas son muy populares en la actualidad ya que eliminan a los competidores falsos y producen ganancias significativas al presupuesto del país del que se trate. La primera vez que se llevó a cabo una subasta fue en Nueva Zelanda en 1989. Debido a la gran emoción que generaron los sistemas móviles 3G, muchos países han incrementado su presupuesto sustancialmente a partir de dichas subastas.

Existen también tres bandas de frecuencia —900 MHz, 2.4 GHz y 5 GHz— recomendadas por el ITU para su uso internacional sin licencia.[1] Dichas bandas están diseñadas para su uso en bienes de propósito general que utilizan comunicaciones inalámbricas (por ejemplo, los dispositivos para cerrar puertas instalados en automóviles); además, algunos dispositivos médicos y científicos también trabajan en este rango. Dichos rangos fueron nombrados así para hacer alusión a estos dispositivos: **industriales, científicos y médicos** (**ISM**). La banda de 900 MHz es la más común y, por ende, la más densamente poblada, lo cual es comprensible, pues a medida que la frecuencia utilizada por un dispositivo específico es mayor, resulta más difícil la tarea de garantizar su bajo costo. Los dispositivos de alta frecuencia son siempre muy costosos. En la actualidad, en la banda de 2.4 GHz se están diseñando muchos usos; por ejemplo, se emplea en nuevas tecnologías como el IEEE 802.11 y Bluetooth. El uso de la banda de 5 GHz apenas ha comenzado. Sin embargo, esta banda parece muy atractiva debido a que garantiza elevadas velocidades para la transmisión de datos.

El requisito obligatorio para el uso compartido de estas bandas es una limitante en la potencia máxima de las señales transmitidas, la cual no debe exceder de 1 W. Esta condición limita el rango de uso del dispositivo, y evita que las señales representen interferencia para otros usuarios que empleen la misma banda de frecuencias dentro de otros distritos de la ciudad.

Existen también métodos de codificación especiales que reducen la interferencia mutua entre los dispositivos que trabajan en las bandas ISM. Dichos métodos se estudiarán con más detalle más adelante.

10.3 SISTEMAS INALÁMBRICOS

PALABRAS CLAVE: líneas de conmutación de radio, comunicaciones por microondas en interiores, puerto infrarrojo incluido, sistema punto a punto, sistema punto-multipunto, sistema multipunto a multipunto, estación base, punto de acceso, panal, celda, entrega, transmisor difuso, comunicaciones satelitales, órbita geoestacionaria (GEO), órbita media terrestre (MEO), órbita baja terrestre (LEO), terminales de muy pequeña apertura (VSAT), sistema de posicionamiento global (GPS), canal intersatelital, sistema Iridium Globalstar y Orbcomm.

10.3.1 Sistema punto a punto

El diseño típico del canal alambrado punto a punto es también popular en las comunicaciones inalámbricas. Diferentes enlaces inalámbricos diseñados con diversos propósitos y que utilizan distintas bandas de frecuencia pueden trabajar mediante el uso de la configuración punto a punto.

[1] Los problemas relacionados con el uso de las bandas de frecuencia de 900 MHz a 5 GHz son que no están libres de licencia en todos los países.

En las redes de transmisión, este diseño se utiliza con frecuencia para construir **líneas de conmutación de radio**. Esta línea generalmente está formada por varias torres sobre las cuales se instalan antenas parabólicas dirigidas (figura 10.5). Cada enlace dentro de dicha línea trabaja en el rango de las microondas a frecuencias de varios gigahertz. Las antenas direccionales concentran su energía en rayos muy angostos, lo cual permite la transmisión de información a distancias considerables (generalmente de hasta 50 kilómetros). Las elevadas torres garantizan la línea de vista directa entre antenas.

El ancho de banda del canal debe ser muy grande. Como regla, varía desde sólo algunos hasta cientos de megabits por segundo. Dichos canales pueden representar tanto troncales como enlaces de acceso (en este último caso, generalmente comprenden sólo un enlace). Los prestadores de servicios de comunicaciones usan con gran frecuencia dichos canales cuando resulta imposible instalar cableado de fibra óptica, debido a condiciones naturales o porque resulte inconveniente desde el punto de vista económico.

El mismo principio de las comunicaciones puede utilizarse dentro de una ciudad para conectar dos edificios. Debido a que no siempre se requiere una elevada velocidad (por ejemplo, puede ser necesario conectar un pequeño segmento de LAN a la LAN principal de la compañía); en este caso, es posible emplear radio módems que operarán en la banda de frecuencia de AM. También es posible usar láseres para conectar dos edificios. Esto garantiza una alta velocidad de la información —hasta 155 Mbps— siempre y cuando las condiciones atmosféricas sean favorables.

Otro ejemplo de un canal inalámbrico punto a punto se muestra en la figura 10.6. En este caso se utiliza para conectar dos computadoras. Dichos canales conforman el segmento más simple de una LAN; por lo tanto, las distancias y la potencia de las señales son básicamente diferentes.

Para las comunicaciones dentro de la misma habitación se puede utilizar una banda infrarroja (figura 10.6*a*) o una banda de microondas (figura 10.6*b*). La mayoría de las computadoras portátiles más recientes están equipadas con puertos infrarrojos, con lo que se permite que dichas conexiones se establezcan de manera automática. Esto sucede siempre y cuando los puertos infrarrojos de las dos computadoras estén en línea de vista o a lo largo de la línea del rayo reflejado.

Las comunicaciones en interiores por microondas operan dentro del rango de las decenas de cientos de metros. No pueden predecirse distancias exactas, ya que una señal de microondas que se propaga dentro de una habitación está sujeta a múltiples casos de reflexión, refracción y dispersión. Esto es independiente de la influencia de ruidos del medio ambiente que penetran las paredes y los paneles de los techos.

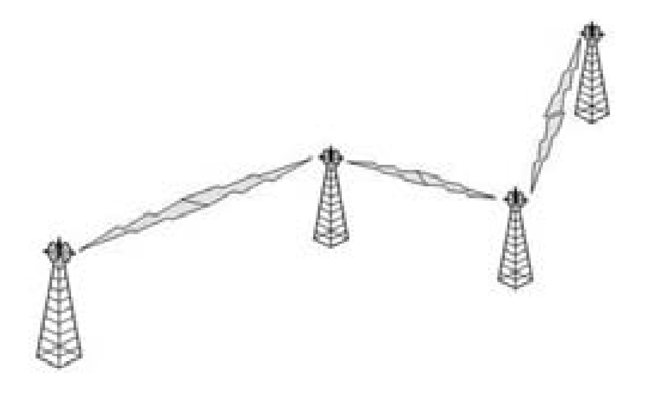


FIGURA 10.5 Canal de radio conmutado.

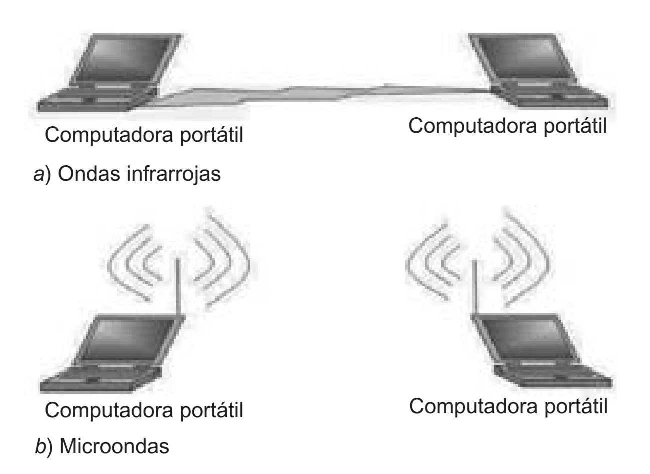


FIGURA 10.6 Comunicaciones inalámbricas entre dos computadoras.

10.3.2 Sistemas punto a multipunto

Este diseño de canal inalámbrico es característico de la administración del acceso cuando múltiples terminales de usuario se conectan a una **estación base**.

Los canales inalámbricos punto a multipunto se utilizan para el acceso fijo y móvil.

La figura 10.7 muestra la variante del acceso fijo cuando se emplean canales de microondas. El prestador de servicios de comunicaciones usa una torre elevada (por ejemplo, una torre de televisión) para garantizar la línea de vista entre las antenas instaladas en las azoteas de los edificios del cliente. En la práctica, esa variante puede ser un conjunto de canales punto a punto, correspondientes al número de edificios que necesitan conectarse a la estación base. Sin embargo, este método representa un desperdicio, ya que por cada nuevo cliente es necesario instalar una nueva antena en una torre. Por ello, con mucha frecuencia se emplean antenas que abarquen sectores específicos (por ejemplo, 45 grados). En este caso, el prestador de servicios puede garantizar las comunicaciones dentro de todo un sector (360 grados) al instalar varias antenas a distancias limitadas una de la otra.

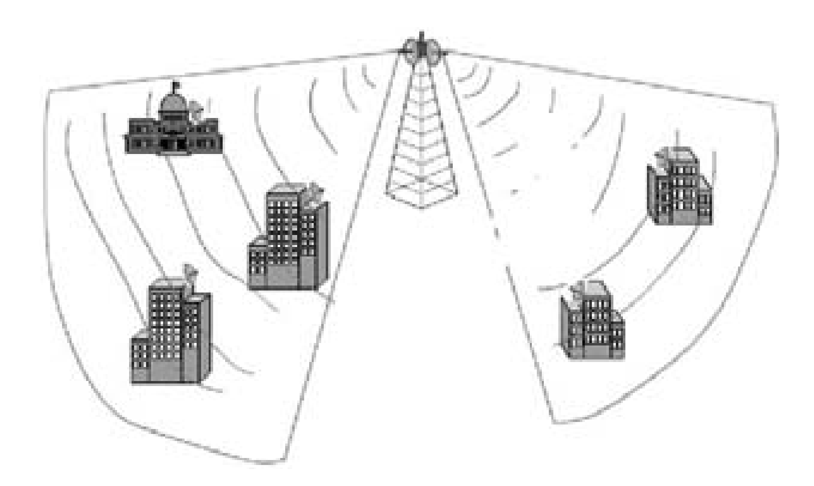


FIGURA 10.7 Acceso inalámbrico fijo.

Los usuarios de canales de acceso pueden intercambiar información con las estaciones base solamente, las cuales, a su vez, sirven como nodos de tránsito para garantizar la comunicación entre los usuarios individuales.

Una estación base por lo general está conectada a la parte guiada de la red, lo cual garantiza la comunicación con los usuarios de otras estaciones base o con los usuarios de las redes guiadas. Debido a lo anterior, a menudo la estación base se llama **punto de acceso**. Con frecuencia, un punto de acceso incluye no sólo el equipo DCE requerido para crear un canal (es decir, para ser un dispositivo de capa física), sino también un teléfono o switch de paquetes. Lo anterior permite al punto de acceso operar como switch de la red a la cual éste proporciona el acceso.

La mayoría de los sistemas de acceso móvil en la actualidad emplean el principio del **panal**, donde cada uno de estos (**celda**) representa un pequeño territorio al que una sola *estación base* brinda servicio. Esta idea no se utilizó inicialmente y los primeros teléfonos móviles no estuvieron basados en ella. Los primeros teléfonos celulares accedían a una sola estación base, abarcando un gran territorio. La idea del uso de pequeñas celdas fue formulada por primera vez en 1945, pero tuvo que pasar un largo tiempo hasta que aparecieran la primeras redes telefónicas celulares comerciales. Los primeros segmentos de prueba aparecieron a finales de la década de 1960 y su uso comercial comenzó a principios de la de 1980.

El principio de dividir todo el territorio cubierto en pequeñas celdas se complementa por la idea de reutilizar frecuencias. La figura 10.8 muestra una variante de la organización de una red celular que usa únicamente tres frecuencias, en las que ningún par de celdas adyacentes emplea la misma frecuencia. La reutilización de frecuencias permite al prestador de servicios usar libremente todo el rango de frecuencias del que posee licencia; al mismo tiempo, los abonados y las estaciones base de las celdas adyacentes no experimentan problemas relacionados de interferencia entre las señales. Como es evidente, la estación base debe controlar la potencia de la señal emitida con la finalidad de evitar la interferencia producida por los efectos del ruido entre dos celdas no adyacentes que utilicen la misma frecuencia.

Cuando las celdas tengan una forma hexagonal, el número de frecuencias reutilizables puede variar. En otras palabras, dicho número no está limitado a tres, como se muestra en la figura 10.8. El número de frecuencias reutilizables (N) puede tener los valores de 3, 4, 7, 9, 12,13, y así sucesivamente.

Dada la mínima distancia entre los centros de dos celdas que utilicen la misma frecuencia, se puede seleccionar N de acuerdo con la fórmula siguiente:

$$N = \frac{D^2}{3R^2} \qquad (10.2)$$

Aquí, R es el radio de la celda y D la distancia de reutilización.

Las pequeñas celdas garantizan tamaños pequeños y una baja potencia del dispositivo terminal del usuario final. Esta circunstancia, así como el progreso tecnológico en general han permitido la creación de teléfonos celulares compactos.

Las redes de computadoras móviles todavía no son tan comunes como las redes telefónicas móviles. No obstante, ambas están basadas en los mismos principios administrativos de los canales inalámbricos.

La transición del dispositivo terminal de una celda a otra es un problema de canales móviles. Este procedimiento, conocido como **entrega**, no existe en el acceso inalámbrico fijo; empero, esta función se relaciona con los protocolos de las capas que se encuentran más arriba de la capa física.

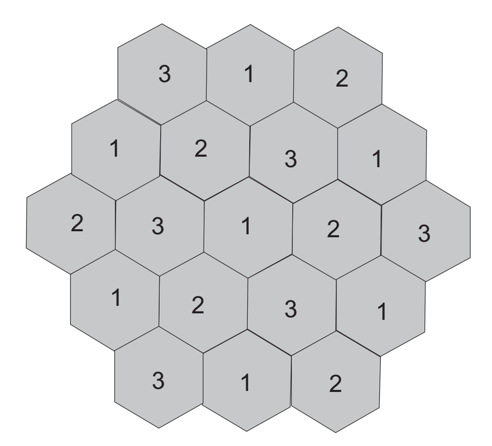


FIGURA 10.8 Reutilización de frecuencias en una red celular.

10.3.3 Sistemas multipunto a multipunto

En este caso, un canal inalámbrico es un medio de transmisión electromagnético compartido por varios nodos. Cada nodo puede utilizar este medio de transmisión para interactuar con cualquier otro nodo sin necesidad de acceder a la estación base. Como no hay ninguna estación base, es necesario hacer uso de un algoritmo descentralizado para acceder al medio de transmisión.

Con mucha frecuencia, los métodos para administrar los canales inalámbricos se usan para conectar computadoras (figura 10.9). Para el tráfico telefónico, la incertidumbre de la parte del ancho de banda que se obtiene en condiciones de medio compartido puede degradar de manera significativa la calidad de la transmisión de la voz. Por lo tanto, las redes

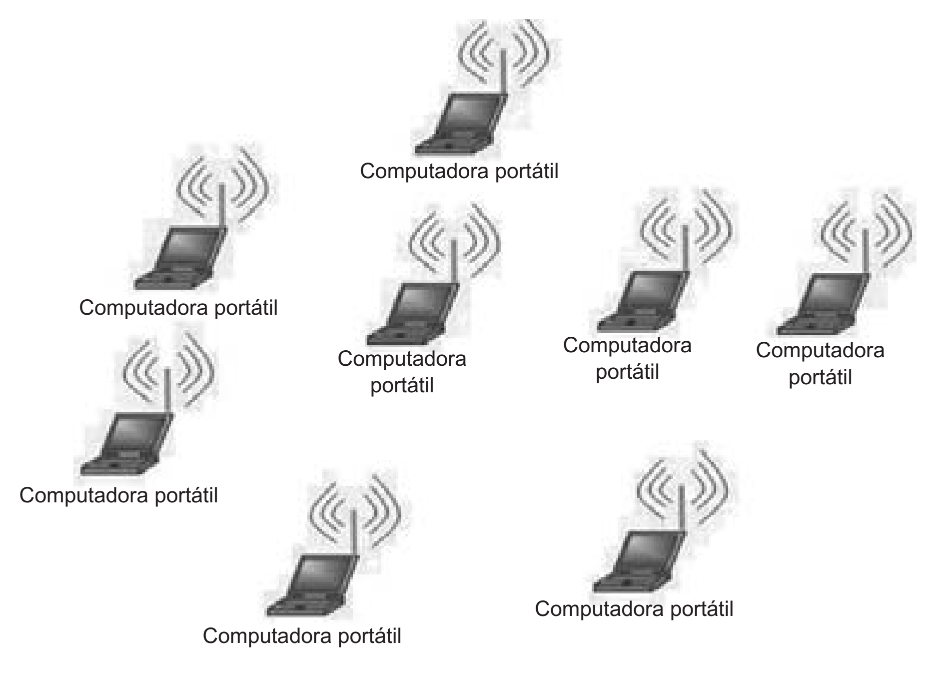


FIGURA 10.9 Canal inalámbrico multipunto a multipunto.

telefónicas siempre usan una estación base para la distribución del ancho de banda (es decir, el método anterior).

La primera LAN diseñada en la década de 1970 en Hawaii correspondió exactamente al diseño que se mostró en la figura 10.9. Dicha LAN difería de las LAN inalámbricas contemporáneas debido a su baja velocidad de comunicación (9 600 bps). Esto, junto con un método de acceso al medio ineficiente, dio como resultado que sólo se utilizara el 18% del ancho de banda de la red.

En la actualidad, tales redes trabajan a velocidades de hasta 52 Mbps en las bandas de las microondas y del infrarrojo. Las antenas omnidireccionales se utilizan en las comunicaciones multipunto a multipunto. Con la finalidad de garantizar la propagación omnidireccional de las ondas infrarrojas, se emplean los **transmisores difusos**, los cuales disipan los rayos mediante el uso de sistemas de lentes.

10.3.4 Sistemas satelitales

Las comunicaciones satelitales se utilizan para administrar canales de microondas de alta velocidad y gran alcance. Estos canales requieren comunicación por línea de vista que no puede garantizarse en grandes distancias debido a la curvatura de la superficie terrestre. El satélite brinda una solución natural a este problema, haciendo las veces de un reflector de señal (figura 10.10).

La idea de usar satélites terrestres artificiales para instalar canales de comunicaciones apareció mucho tiempo antes de que la Unión Soviética lanzara su primer satélite en 1957. Arthur C. Clarke continuó y desarrolló más allá la obra de Jules Verne y H.G. Wells, quien describió muchas invenciones técnicas antes de que fueran implementadas. En su artículo titulado "Conmutadores extraterrestres", publicado en 1945, Clarke describió un satélite estacionario suspendido sobre un punto específico sobre el ecuador, con el cual se garantizaban las comunicaciones en la mayor parte de la superficie terrestre.

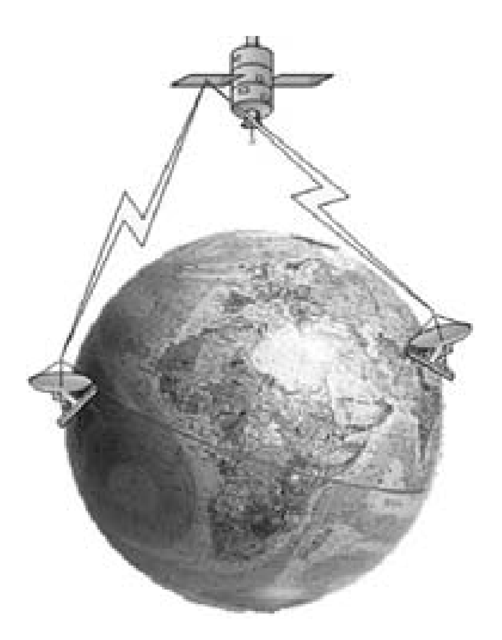


FIGURA 10.10 El satélite como reflector de señales.

El primer satélite lanzado por la Unión Soviética durante la Guerra Fría no fue un satélite estacionario y brindaba capacidades de comunicación muy limitadas. De hecho, sólo transmitía la señal de radio bip-bip con el fin de alertar a la gente en todo el mundo acerca de su presencia en el espacio exterior. Sin embargo, este éxito de la hoy desaparecida Unión Soviética obligó a Estados Unidos a tratar de alcanzar la delantera tecnológica. En 1962 se lanzó el primer satélite de telecomunicaciones estadounidense, llamado *Telstar I*, que soportaba 600 canales de voz.

Han transcurrido más de 40 años desde que se lanzó el primer satélite de comunicaciones y las funciones de dichos satélites se han hecho cada vez más complejas, como es natural. En la actualidad, un satélite trabaja como un nodo en una red de transmisión, como un switch telefónico o como un switch o ruteador de una red de computadoras. Hoy en día, el equipo satelital es capaz de interactuar tanto con estaciones terrenas como con equipo instalado en otros satélites, formando así canales inalámbricos directos en el espacio. No existen diferencias importantes entre las técnicas de transmisión de señales de microondas en el espacio y sobre la superficie terrestre. No obstante, los canales satelitales tienen características específicas: uno de los nodos que forman dicho canal vuela constantemente a una distancia significativa respecto a los demás nodos.

La ITU ha reservado varias bandas de frecuencia para las comunicaciones satelitales (tabla 10.1).

La banda **C** fue la primera que se utilizó. En esta banda se reservaron 500 MHz para cada flujo dúplex Tierra-satélite (frecuencia de subida) y satélite-Tierra (frecuencia de bajada), la cual es suficiente para administrar un gran número de canales. Las bandas **L** y **S** se usan para administrar servicios móviles que emplean satélites. Con mucha frecuencia, también se utilizan en sistemas terrestres. A su vez, las bandas **Ku** y **Ka** no están muy pobladas sobre la Tierra en la actualidad, por una razón: el alto costo del equipo evita que la mayoría de las compañías usen esta banda, lo cual es particularmente cierto para la banda Ka.

Los satélites artificiales orbitan la Tierra de acuerdo con las leyes descubiertas por Johannes Kepler. En general, la órbita satelital es elíptica. Sin embargo, para mantener un peso constante sobre la superficie de la Tierra, se puede seleccionar una órbita circular.

En la actualidad se usan los tres grupos siguientes de órbitas circulares, los cuales difieren en cuanto a su distancia respecto a la superficie terrestre (figura 10.11).

Órbita geoestacionaria o GEO (35 863 km)
Órbita media terrestre o MEO (5 000-15 000 km)
Órbita baja terrestre o LEO (100-1 000 km)

TABLA 10.1 Bandas de frecuencia asignadas por la ITU para las comunicaciones satelitales

Banda	Frecuencia de bajada (GHz)	Frecuencia de subida (GHz)
L	1.5	1.6
S	1.9	2.2
C	3.7-4.2	5.925-6.425
Ku	11.7-12.1	14.0-14.5
Ka	17.7-21.7	27.5-30.5

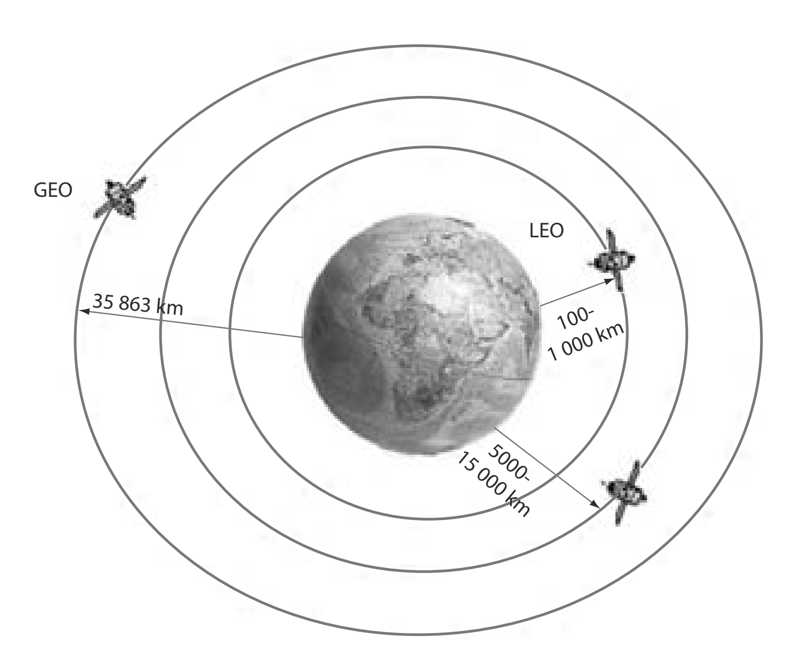


FIGURA 10.11 Tipos de órbitas satelitales.

10.3.5 Satélite geoestacionario

Un **satélite geoestacionario** está suspendido en algún punto del ecuador, y viaja a la misma velocidad de rotación de la Tierra. Esta posición es conveniente por las razones que siguen: primera, un cuarto de la superficie terrestre está dentro de su línea de vista en todo momento. Por lo tanto, si se utilizan satélites geoestacionarios, será fácil administrar la *difusión amplia dentro de todo un país o, aún más, dentro de todo un continente.*

Segunda, el satélite representa un punto fijo para las antenas en la Tierra, lo cual simplifica mucho el proceso de administración de las comunicaciones. De hecho, elimina la necesidad de corregir de manera automática la dirección de la antena terrestre (en contraste con los satélites MEO y LEO). Esta situación cambió con la llegada de las antenas omnidireccionales de tamaño reducido en la década de 1990: ahora no es necesario rastrear continuamente la posición de los satélites LEO, sino que basta garantizar que el satélite esté en la línea de vista.

Tercera, un satélite geoestacionario orbita sobre la atmósfera de la Tierra y, por lo tanto, sufre un menor desgaste que los satélites MEO y LEO. Los satélites LEO, debido a su resistencia al aire, pierden peso de modo constante, el cual deben corregir mediante el uso periódico de motores.

Los satélites geoestacionarios por lo regular soportan muchos canales debido a sus distintas antenas.

Como regla, el uso de satélites GEO se relaciona con el uso de grandes antenas con diámetros de alrededor de 10 metros. Esto complica el uso de satélites GEO por pequeñas organizaciones y personas. Pero la situación ha cambiado con el desarrollo de antenas dirigidas instaladas en los satélites, las cuales generan señales que pueden ser recibidas mediante el uso de antenas terrestres relativamente pequeñas, conocidas como terminales de apertura muy pequeña (VSAT). El diámetro de una VSAT es de alrededor de un metro. Las estaciones

terrestres equipadas con VSAT en la actualidad soportan una amplia gama de servicios, como telefonía, transmisión de datos y conferencias.

A pesar de lo anterior, los satélites geoestacionarios no se salvan de tener desventajas. La más evidente es su enorme distancia respecto a la superficie terrestre, que resulta en retardos de propagación significativos que van desde 230 hasta 280 mseg. Cuando se utilizan tales satélites para transmitir una conversación o una teleconferencia, se presentan pausas que interfieren con la transmisión normal.

Asimismo, a semejantes distancias las pérdidas en la señal son elevadas, lo cual significa que es necesario utilizar poderosos transmisores y antenas de grandes diámetros. Esto no tiene que ver con las VSAT, pero cuando se usan, la cobertura se reduce.

La principal desventaja de un satélite geoestacionario con su órbita circular es la pobre calidad de comunicación para las regiones cercanas a los polos norte y sur. Las señales para dichas regiones viajan una distancia mayor que las que se envían a las regiones ecuatoriales y a latitudes bajas o moderadas; en consecuencia, éstas sufren una atenuación mucho mayor. Una buena solución a este problema reside en lanzar un satélite con una órbita elíptica pronunciada, la cual esté cercana a la Tierra en las regiones correspondientes a los polos norte y sur.

La ITU también regula las posiciones de los satélites geoestacionarios en sus órbitas. En estos días existe una gran escasez de dichas posiciones debido a que los satélites GEO no pueden estar a una distancia más cercana a 2 grados, uno respecto al otro en la órbita. Esto significa que en cada órbita no puede haber más de 180 satélites similares. Como no todos los países pueden lanzar un satélite GEO, la situación es semejante a la competencia por una banda de frecuencia específica. En este caso, sin embargo, la competencia es todavía más intensa debido a las ambiciones políticas de los países que participan.

10.3.6 Satélites de órbita terrestre baja y media

La clase MEO de satélites no es actualmente tan popular como la GEO y la LEO. Los satélites MEO garantizan un diámetro de cobertura que va desde los 10 000 hasta los 15 000 km y un retardo de propagación de la señal de 50 mseg. El servicio más conocido y popular ofrecido por los satélites MEO es el **sistema de posicionamiento global** (GPS). El *GPS* es un sistema global para determinar las coordenadas actuales de un usuario sobre la superficie terrestre o dentro del espacio cercano a la Tierra. El GPS está formado por 24 satélites, una red especial basada en tierra para rastrearlos y un número ilimitado de dispositivos terminales (receptores). Mediante el uso de señales de radio desde los satélites, los receptores GPS constantemente (y de manera muy precisa) determinan las coordenadas actuales de la ubicación de un usuario. Como regla, los errores nunca exceden las decenas de metros. Esto es más que suficiente para resolver problemas de navegación, como el movimiento de objetos (aviones, barcos, automóviles, etcétera).

Los satélites LEO poseen diferentes ventajas y desventajas respecto a los satélites geoestacionarios. Su ventaja principal es la proximidad con la Tierra. En consecuencia, requieren una potencia reducida en los transmisores, de pequeñas antenas y de un tiempo de propagación corto de la señal (de 20 a 25 mseg); además, son más fáciles de lanzar. La principal desventaja es su pequeña área de cobertura (sólo de alrededor de 8 000 km de diámetro). Este satélite gira alrededor de la Tierra en un tiempo de 1.5 a 2 horas y es visible a la estación terrena por un tiempo muy corto: 20 minutos solamente. Esto significa que la comunicación continua mediante el uso de LEO podrá garantizarse sólo si un número suficiente de estos satélites se lanzan a la órbita. Además, la resistencia atmosférica reduce la vida útil de dichos satélites a ocho o 10 años.

En contraste con los satélites GEO, que están diseñados principalmente para la difusión amplia y las comunicaciones fijas a larga distancia, los satélites LEO se consideran medios importantes para soportar las comunicaciones móviles.

A principios de la década de 1990, los ejecutivos de Motorola evaluaron las ventajas de los dispositivos terminales de los satélites LEO. En cooperación con algunos de sus socios más grandes, esta compañía comenzó el proyecto *Iridio*, cuyo objetivo principal era muy ambicioso: crear una red satelital a nivel mundial que garantizara las comunicaciones móviles en cualquier punto geográfico de la Tierra. A finales del decenio de 1980, el sistema celular de telefonía móvil no era tan denso como lo es ahora. Por ende, su éxito comercial parecía estar garantizado.

En 1997, el sistema de 66 satélites se lanzó y la operación comercial del sistema Iridio comenzó en 1998. Los satélites Iridio cubren toda la superficie de la Tierra girando en seis órbitas que pasan sobre los polos. En cada órbita existen 11 satélites equipados con transmisores a frecuencias de 1.6 GHz y un ancho de banda de 10 MHz. Tal ancho de banda se utiliza para administrar 240 canales de 41 KHz cada uno. Gracias a la reutilización de frecuencias, el sistema Iridio soporta 253 440 canales, con lo cual administra el sistema de celdas a lo largo de la superficie terrestre. Los principales servicios que brinda Iridio a sus usuarios son las comunicaciones telefónicas (a $7 por minuto) y la transmisión de datos a 2.4 Kbps.

Los satélites Iridio se caracterizan por su comportamiento intelectual; por ejemplo, éstos pueden usar canales intersatelitales especiales para intercambiar información a una velocidad de 25 Mbps. Por lo tanto, una llamada telefónica desde el teléfono satelital Iridio se transmite en forma directa hacia el satélite que tiene a línea de vista en ese momento. Después este satélite envía la llamada, utilizando el sistema de satélites de tránsito, al satélite que esté más cercano al abonado que es llamado. El sistema Iridio es una red con una pila de protocolos propietaria completa desde el punto de vista funcional que garantiza el rastreo a nivel mundial.

Por desgracia, el éxito comercial de Iridio fue modesto y la compañía fue a la quiebra después de dos años de existencia. Sus pronósticos acerca de la viabilidad de los abonados telefónicos móviles demostraron ser erróneos. Cuando su sistema había comenzado sus operaciones comerciales, una red de telefonía celular basada en tierra ya había cubierto los países industriales. Al mismo tiempo, los servicios que aseguraban la transmisión de datos a 2.4 Kbps no cumplieron con los requerimientos de los usuarios a finales del siglo XX.

En la actualidad, el sistema Iridio ha sido puesto en operación otra vez, pero tiene un nuevo dueño y una nueva marca: Iridio Satellite. Por el momento, éste tiene un plan modesto relacionado con la creación de sistemas locales para las comunicaciones móviles en aquellas partes del mundo que no cuentan prácticamente con sistemas de comunicaciones. El software de los satélites está siendo actualizado y modificado de manera casi espontánea, lo cual permite que la velocidad de transmisión de datos sea elevada a 10 Kbps.

El sistema Globalstar constituye otra red satelital LEO muy popular. En contraste con Iridio, los 48 satélites LEO del sistema Globalstar realizan funciones de repetidor convencionales. Dichos satélites reciben llamadas telefónicas de abonados móviles y las transmiten a la estación base terrestre más cercana. La estación base lleva a cabo el enrutamiento de las llamadas al transferir la llamada entrante al satélite más cercano. El abonado llamado se ubica en su línea de vista y los canales intersatelitales no se utilizan. Además de las comunicaciones telefónicas, Globalstar también transmite datos a 4.8 Kbps.

Otra red LEO es Orbcomm, que ofrece servicios orientados a la transmisión de datos. Desafortunadamente, la entrega de mensajes no se lleva a cabo en tiempo real. Si el satélite no está visible, la terminal Orbcomm sólo memorizará los paquetes hasta que el satélite ingrese otra vez a la zona de línea de vista. Como resultado, la transferencia de datos es muy

irregular. En lugar de que los retardos duren fracciones de segundo, a lo cual la mayoría de los usuarios de Internet están acostumbrados, los retardos de esta red pueden ser de varios minutos.

En la actualidad, ahora que es evidente que la telefonía móvil estará soportada en lo fundamental por redes celulares basadas en tierra, la mayoría de los sistemas satelitales están cambiando su orientación. El ofrecimiento de un rápido acceso a Internet pasa a ocupar un primer plano. Uno de dichos sistemas es Teledesic, entre cuyos fundadores está el creador de Microsoft, Bill Gates. En este sistema, que comenzó a desarrollarse a principios de la década de 1990, los satélites son ruteadores con una total funcionalidad, conectados a través de canales intersatelitales de 64 Mbps.

Los sistemas de acceso a Internet basados en satélites GEO —Spaceway, Astrolink y Euro-Skyway— también están en etapa de construcción. Tales sistemas están orientados hacia el uso de terminales VSAT y prometen brindar a sus usuarios canales de acceso a 2-20 Mbps.

10.4 TECNOLOGÍA DE ESPECTRO DISPERSO

PALABRAS CLAVE: tecnología de espectro disperso, inmunidad al ruido, congestión de señales de radio, multiplexaje por división de frecuencia ortogonal (OFDM), espectro disperso con salto de frecuencia (FHSS), secuencia de salto, FHSS lento, FHSS rápido, IEEE 802.11, Bluetooth, espectro disperso de secuencia directa (DSSS), trozo, periodo del trozo, velocidad de trozos, y acceso multiplexado por división de código (CDMA).

La tecnología de espectro disperso ha sido diseñada de manera especial para la transmisión inalámbrica. Permite mejorar la inmunidad al ruido del código para señales de baja potencia, el cual es de importancia significativa en las aplicaciones móviles. Sin embargo, es esencial observar que la técnica de espectro disperso no es la única de codificación empleada en canales inalámbricos de la banda de microondas. Todos los tipos de FSK y PSK descritos en el capítulo 9 también se utilizan. El ASK no se usa debido a que los canales de microondas tienen un gran ancho de banda y los amplificadores que garantizan el mismo coeficiente de amplificación para un amplio rango de frecuencias son muy costosos.

El gran ancho de banda también facilita utilizar la modulación de multisubportadora en la que el ancho de banda se divide en varios subcanales, cada uno de los cuales emplea una frecuencia portadora específica. De acuerdo con esto, la ráfaga de bits se divide en varias subráfagas de velocidades menores. Después, cada subráfaga se modula con el uso de una subportadora específica, por lo general un múltiplo de la primera frecuencia subportadora (es decir, f_0, $2f_0$, $3f_0$, y así sucesivamente). La modulación se lleva a cabo por medio de métodos estándar de FSK o PSK. Esta técnica se conoce con el nombre de **multiplexaje por división de frecuencia ortogonal** (**OFDM**).

Antes de transmitir, todas las subportadoras se convolucionan matemáticamente en una señal común al utilizar la transformada rápida de Fourier. El espectro de dicha señal es casi igual al espectro de la señal codificado empleando una sola portadora. Después de la transmisión, la transformada inversa de Fourier se usa para detectar los subcanales de la portadora; después, una ráfaga de bits se recibe de cada canal. La ganancia que resulta de dividir la ráfaga de bits a alta velocidad de la fuente en varias ráfagas de baja velocidad se manifiesta en sí misma en un aumento en el intervalo entre los símbolos individuales del código. Esto significa que el efecto de la interferencia intersimbólica debido a la propagación multitrayectoria de las ondas electromagnéticas se reduce.

10.4.1 Espectro disperso con salto de frecuencia

La idea de contar con **un** espectro disperso apareció durante la Segunda Guerra Mundial, cuando la radio se utilizaba por lo común para llevar a cabo negociaciones secretas, así como para controlar objetos militares, como torpedos. Para evitar la fuga o congestión de las señales de radio con ruido de banda angosta, las transmisiones de radio se llevaban a cabo cambiando constantemente la frecuencia de la portadora dentro de un amplio rango de frecuencias. Como resultado, la potencia de la señal fue distribuida en todo el rango y escuchar una frecuencia específica producía sólo un pequeño ruido insignificante. La secuencia de las frecuencias portadoras se seleccionó como seudoaleatoria y solamente la conocían el transmisor y el receptor. Los intentos para suprimir la señal dentro de una banda angosta específica no afectaron de modo adverso a la señal dispersa, pues sólo se eliminaba una pequeña parte de la información.

El concepto de este método, conocido como **espectro disperso con salto de frecuencia** (**FHSS**), se muestra en la figura 10.12.

Los intervalos durante los cuales la transmisión continúa a la misma frecuencia de la portadora se conocen como periodos de trozo. Sobre cada frecuencia portadora se utilizan métodos estándares de modulación como FSK o PSK para transmitir información discreta. Para sincronizar el receptor con el transmisor, al comienzo de cada periodo de trozo se asigna un intervalo específico para transmitir varios bits de sincronización. Por lo tanto, la velocidad efectiva de este método de codificación es menor debido al tiempo desperdiciado en enviar la información de sincronización.

La frecuencia de la portadora cambia constantemente de acuerdo con los números de los subcanales de frecuencia producidos por el generador de números seudoaleatorios. La secuencia seudoaleatoria depende de un parámetro específico conocido con el nombre de semilla. Siempre y cuando tanto el transmisor como el receptor conozcan el valor de la semilla, éstos cambiarán las frecuencias de acuerdo con la misma secuencia. La secuencia de acuerdo con la cual las frecuencias de las portadoras son cambiadas se llama **secuencia de salto**.

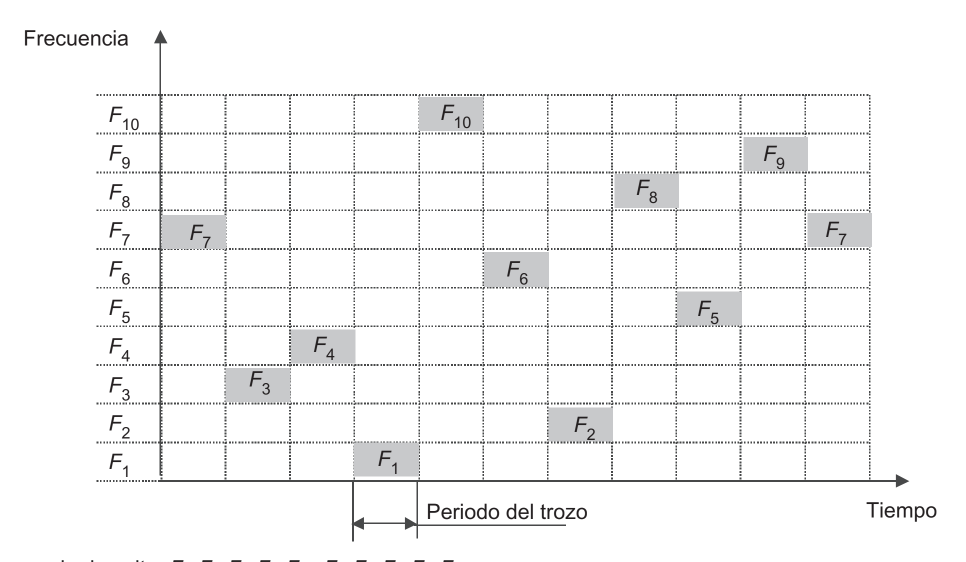


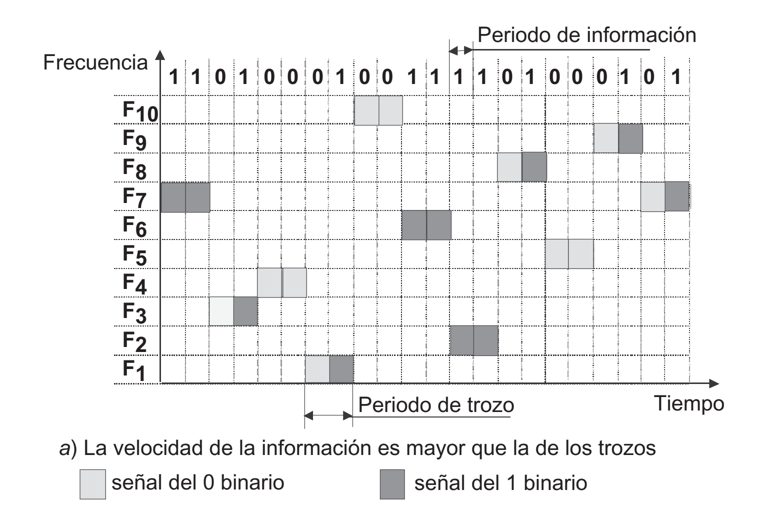
FIGURA 10.12 Dispersión del salto de frecuencias.

La frecuencia a la cual las frecuencias de los subcanales son cambiadas se conoce con el nombre de **velocidad de trozo**. Si dicha velocidad es menor que la velocidad de información del canal, a este modo de operación se le llama *FHSS lento* (figura 10.13*a*). Por lo demás, encontrará principalmente el *FHSS rápido* (figura 10.13*b*).

El FHSS rápido garantiza una mejor inmunidad al ruido; la supresión de ruido de banda angosta de una señal en un subcanal específico no resulta en una pérdida de bits, ya que este valor de bits se repite varias veces en diferentes subcanales y sólo una copia de este valor se distorsiona. De este modo, la interferencia intersimbólica no se presenta debido a que cuando una señal llega, al haber sido retrasada a lo largo de una de las rutas, el sistema ya tuvo tiempo suficiente para desplazarse hacia otra frecuencia.

El FHSS lento no tiene esta propiedad, a pesar de que es mucho más fácil de implementar y se caracteriza por un menor número de bits extra.

Los métodos FHSS se emplean en tecnologías inalámbricas, como el IEEE 802.11 y Bluetooth.



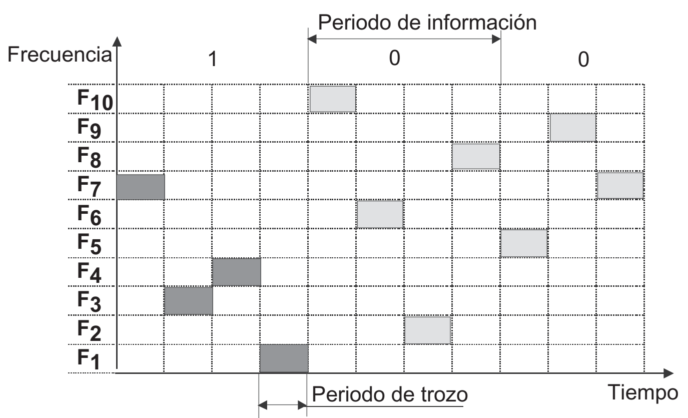


FIGURA 10.13 Relación entre la velocidad de la información y la velocidad de trozos.

La forma FHSS que utiliza la banda de frecuencia es diferente de las que emplean otros métodos de codificación. En vez de reservar el uso de una banda de frecuencia angosta, el FHSS trata de usar todo el rango disponible. Al principio, podría parecer que este método se encuentra muy lejos de ser eficaz, pues en cualquier momento sólo trabaja un canal. Pese a lo anterior, éste no es un supuesto preciso, ya que los códigos de espectro disperso también pueden utilizarse para multiplexar varios canales dentro de un amplio rango. En particular, el FHSS permite administrar la operación de varios canales mediante la selección de secuencias seudoaleatorias para cada canal con el fin de garantizar que, en cualquier momento, cada canal trabaje a una frecuencia diferente. Lo anterior podrá lograrse sólo si el número de canales no excede la cantidad de subcanales disponibles.

10.4.2 Espectro disperso de secuencia directa

El **método de espectro disperso de secuencia directa** (**DSSS**) también utiliza la banda de frecuencias completa asignada para un solo enlace inalámbrico. No obstante, la técnica que utiliza para lograr lo anterior difiere de la que emplea el FHSS. El DSSS usa todo el rango asignado a éste, pero al hacerlo no conmuta frecuencias constantemente. En este caso, cada bit de información es reemplazado por N bits, de tal manera que la velocidad de transmisión de la señal se incrementa N veces; a su vez, esto significa que el espectro de la señal también aumenta N veces. Por lo tanto, basta con seleccionar de manera adecuada la velocidad de información, así como el valor de N para que el espectro de la señal se extienda a través de todo el rango.

El objetivo de la codificación DSSS es el mismo que el de la codificación FHSS, es decir, mejorar la inmunidad al ruido. El ruido de banda angosta podría distorsionar solamente frecuencias específicas del espectro de la señal. Por ende, existe una alta probabilidad de que el receptor reconozca de manera acertada la información transmitida.

El código utilizado para reemplazar un bit de la información de origen se conoce como secuencia de dispersión y cada bit de dicha secuencia se llama **trozo**. De acuerdo con esto, la velocidad de transmisión del código resultante se conoce como velocidad de trozo. El cero binario se codifica a través del valor inverso de la secuencia de dispersión. Los receptores deben conocer el valor de la secuencia de dispersión que utilizaron los transmisores para reconocer correctamente la información transmitida.

El número de bits en una secuencia de trozo es el factor de dispersión, pues define el coeficiente de expansión del código fuente. De la misma manera que con el FHSS, cualquier tipo de modulación (por ejemplo, BFSK) puede utilizarse para codificar bits del código resultante.

A medida que el valor del factor de dispersión sea más grande, el espectro de la señal resultante será más ancho y el nivel de supresión del ruido más alto. La banda del espectro consumida por la señal también será mayor. En general, el factor de dispersión toma los valores de 10 a 100.

Un ejemplo de la secuencia de dispersión es la llamada secuencia de Barker, la cual comprende los 11 bits: 10110111000. Si un transmisor utiliza esta secuencia, la transmisión de tres bits 110 resultará en la transmisión de los bits siguientes:

10110111000 10110111000 01001000111

La secuencia de Barker permite que el receptor se sincronice en forma rápida a nivel símbolo con el transmisor (es decir, detectar de manera confiable el punto de comienzo de la secuencia). El receptor detecta dicho evento al comparar secuencialmente los bits recibidos con el patrón de la secuencia. Si la secuencia de Barker se compara con el mismo patrón

desplazado 1 bit a la derecha o a la izquierda, coincidirán menos de la mitad de los bits. Esto significa que aun si varios bits estuvieran distorsionados, el receptor determinaría de manera correcta el punto de comienzo de la secuencia con una alta probabilidad. Por ello, el receptor podría interpretar con acierto la información recibida.

El DSSS está menos protegido contra el ruido que el FHSS rápido, ya que el ruido de gran potencia de banda angosta influye en parte del espectro y, por ende, en los resultados del reconocimiento de unos y ceros.

10.4.3 Acceso múltiple por división de código

De la misma manera que FHSS, la codificación DSSS permite que haya multiplexaje de varios canales dentro de la misma banda. La técnica de tal multiplexaje se llama **acceso multiplexado por división de código** (**CDMA**), se utiliza ampliamente en las redes celulares y puede emplearse con los métodos de codificación FHSS y DSSS. En la práctica se usa con mayor frecuencia cuando las redes inalámbricas utilizan códigos DSSS.

En una red que emplea CDMA, cada nodo envía datos al medio de transmisión compartido en cualquier momento que lo requiera, lo cual significa que no existe sincronización entre los nodos de la red. La idea de CDMA consiste en que cada nodo de la red use su propio valor de la secuencia de dispersión. Los valores de la secuencia se seleccionan para garantizar que el nodo receptor conozca que la secuencia de dispersión del nodo transmisor puede seleccionar los datos del nodo transmisor a partir de la señal creada como resultado de la transmisión simultánea de información por varios nodos.

Para garantizar que dicha operación de demultiplexaje pueda realizarse, los valores de la secuencia de dispersión se seleccionan de una forma especial. A continuación se tratará de explicar CDMA por medio de un ejemplo.

Suponga que existen cuatro nodos en la red: A, B, C y D. Cada nodo utiliza su propio valor de secuencia de dispersión:

A: 0 0 0 0
B: 0 1 0 1
C: 0 0 1 1
D: 0 1 1 0

Suponga también que cuando los unos y ceros transmitidos emplean una secuencia de dispersión (código fuente transformado) se usan las señales inversa y aditiva. La propiedad de inversión significa que el uno binario, por ejemplo, se codifica mediante una senoidal de amplitud +A; el cero binario se codifica por medio de una senoide de amplitud –A. A partir de la propiedad aditiva, se deduce que si las fases de dichas senoidales coinciden, la señal será de nivel 0 cuando se transmitan de manera simultánea el uno binario y el cero binario. Para simplificar la escritura de la secuencia de dispersión, designe la senoidal con amplitud positiva como +1 y la senoidal con amplitud negativa como –1. Para efectos de simplificación, suponga que todos los nodos están sincronizados.

De esta manera, cuando se transmita el bit uno del código fuente, los cuatro nodos trasmitirán las siguientes secuencias a través del medio de transmisión:

A: –1 –1 –1 –1
B: –1 +1 –1 +1
C: –1 –1 +1 +1
D: –1 +1 +1 –1

Cuando se transmita un bit cero del código fuente, se invertirán las señales de la secuencia de dispersión.

Ahora, suponga que cada uno de los cuatro nodos transmite 1 bit de la información de la fuente independientemente de los demás nodos; el nodo A transmite un bit fijado a 1, el nodo B transmite un bit fijado a 0, el nodo C transmite un bit fijado a 0 y el nodo D transmite un bit fijado a 1.

La siguiente secuencia de señales se transmitirá al medio de transmisión de la red (S):

A: –1 –1 –1 –1
B: +1 –1 +1 –1
C: +1 +1 –1 –1
D: –1 +1 +1 –1

De acuerdo con la propiedad aditiva:

S: 0 0 0 –4

Suponga que el nodo E necesita recibir información proveniente del nodo A. Para recibirla, tiene que utilizar su demodulador CDMA especificándole a éste la secuencia de dispersión del nodo A como un parámetro.

El demodulador CDMA opera como sigue: suma de manera secuencial las cuatro señales totales (*Si*) recibidas durante cada pulso de reloj. La señal *Si* recibida durante el pulso de reloj cuando el código de dispersión del nodo A es +1 se toma en cuenta con su signo, y la señal recibida durante el pulso de reloj cuando el código de dispersión del nodo A es –1 se adiciona a la suma con el signo invertido. En otras palabras, el demodulador calcula el producto escalar del vector de las señales recibidas y el vector de los valores de la secuencia de dispersión del nodo requerido:

$$S \times \mathrm{A} = (0\ 0\ 0\ {-4}) \times (-1\ {-1}\ {-1}\ {-1}) = 4$$

Para encontrar qué bit fue enviado por el nodo A, el resultado debe estar normalizado, por ejemplo: al dividir entre el número de nodos de la red: 4/4 = 1.

Si el nodo E debe recibir información del nodo B, tiene que utilizar el código de dispersión del nodo para remodular o B(–1+1–1+1):

$$S \times B = (0\ 0\ 0\ {-4}) \times (-1\ {+1}\ {-1}\ {+1}) = -4.$$

Después de normalizar, recibimos la señal –1, la cual corresponde al cero binario de la información fuente del nodo B.

Una característica de las secuencias de dispersión utilizadas en CDMA es que éstas son mutuamente ortogonales, lo cual significa que si usted las considera vectores, éstas generarán un 0 cuando se multipliquen por pares. Los vectores (1 0 0), (0 1 0) y (0 0 1) del espacio tridimensional constituyen otro ejemplo de vectores mutuamente ortogonales. No obstante, para utilizar vectores en CDMA, es necesario garantizar que éstos sean no sólo mutuamente ortogonales, sino también ortogonales respecto a los miembros invertidos del conjunto de vectores. Esto se debe a que los miembros invertidos se utilizan para codificar los ceros de la información fuente.

Aquí se ha explicado sólo la idea fundamental del CDMA, tratando de resumir la situación tanto como fue posible. En la práctica, CDMA es una tecnología simplificada que no trabaja con +1 y –1 convencionales; en lugar de eso, opera con señales moduladas, como las señales BPSK. Además, los nodos de la red no se sincronizan. Por último, las señales que llegan de los nodos ubicados a diferentes distancias respecto al receptor tienen potencias diversas. El problema de la sincronización entre el receptor y el transmisor se resuelve mediante el envío

de una larga secuencia de código predefinido conocida como *señal piloto*. Con el fin de hacer que las potencias de todos los transmisores sean vistas por la estación base como aproximadamente iguales, el CDMA utiliza procedimientos especiales para controlar la potencia.

RESUMEN

- Las comunicaciones inalámbricas se clasifican en categorías inalámbricas fijas e inalámbricas móviles. Para administrar las comunicaciones móviles, no existe más alternativa que el medio inalámbrico. Las comunicaciones inalámbricas fijas garantizan el acceso a los nodos de red ubicados dentro de los límites de un área pequeña (por ejemplo, un edificio).
- Cada nodo del canal de comunicaciones inalámbricas está equipado con una antena, la cual transmite y recibe ondas electromagnéticas de manera simultánea.
- Las ondas electromagnéticas se pueden propagar en todas direcciones (omnidireccionales) o dentro de cierto sector (direccionales). El tipo de propagación depende del tipo de antena.
- Los sistemas de transmisión de datos inalámbricos encajan dentro de los cuatro grupos siguientes en función del rango del espectro electromagnético que utilicen:
  - Sistemas de radio (difusión)
  - Sistemas de microondas
  - Sistemas de ondas infrarrojas
  - Sistemas de luz visible
- Debido a la reflexión, difracción y dispersión de las ondas electromagnéticas, se presentan efectos de la propagación multitrayectoria en la señal. Esto provoca la presencia de interferencia intersimbólica y el desvanecimiento multitrayectoria.
- La transmisión de datos en las bandas de 900 MHz, 2.4 GHz y 5 GHz, llamadas bandas industriales, científicas y médicas, no requiere licencias siempre y cuando la potencia transmitida no exceda de 1 W.
- Los canales inalámbricos punto a punto se usan para la creación de líneas de conmutación de radio para la comunicación entre edificios y pares de computadoras.
- Los canales inalámbricos punto a multipunto se forman de acuerdo con la estación base. Dichos canales se utilizan en redes celulares móviles y en sistemas con acceso fijo.
- La topología multipunto a multipunto es característica de las LAN inalámbricas.
- Los sistemas de telecomunicaciones por satélite utilizan tres grupos de órbitas circulares que difieren en su distancia respecto a la superficie terrestre:
  - Órbita geoestacionaria (35 863 km)
  - Órbita media terrestre (5 000-15 000 km)
  - Órbita baja terrestre (100-1 000 km)
- Para codificar información discreta, los sistemas inalámbricos utilizan los siguientes tipos de modulación:
  - FSK y PSK
  - Modulación OFDM con varias frecuencias de portadora
  - Métodos de espectro disperso-espectro disperso con salto de frecuencia (FHSS) y espectro disperso de secuencia directa (DSSS).

- Los métodos de espectro disperso usan un rango de frecuencias para representar información. Éste reduce la influencia de ruido de banda angosta de las señales.
- Basados en FHSS y DSSS, es posible multiplexar varios canales dentro de la misma banda de frecuencia. Esta técnica de multiplexaje se conoce como acceso múltiple por división de código.

PREGUNTAS DE REPASO

1. Elabore una lista de las áreas principales de aplicación de los canales de comunicación inalámbricos.
2. ¿Cuáles son las ventajas y limitaciones de la transmisión inalámbrica de información comparada con los métodos de transmisión que utilizan medios guiados?
3. ¿Cómo se puede administrar la propagación omnidireccional de ondas de radio y de microondas?
4. ¿Qué factores permiten que las ondas de radio de frecuencias en el rango de 2 a 30 MHz se propaguen a cientos de kilómetros?
5. ¿Qué espectro se utiliza en las comunicaciones satelitales?
6. ¿Qué condiciones atmosféricas impiden la propagación de las microondas?
7. ¿Qué dispositivos se emplean en la propagación omnidireccional de ondas infrarrojas?
8. ¿Qué barreras provocan la difracción de ondas electromagnéticas?, ¿cuáles provocan esparcimiento?
9. ¿Cuándo es necesario usar órbitas elípticas en los satélites de comunicaciones?
10. ¿Cuáles son las desventajas de los satélites geoestacionarios?
11. En su opinión, ¿cuáles son las razones del fracaso comercial del proyecto Iridio?
12. ¿Qué condición debe tenerse en cuenta para que la tecnología FHSS sea rápida?
13. ¿Qué propiedad de la secuencia de Barker es la razón de su uso en la tecnología DSSS?
14. ¿Cuál es la propiedad principal de las secuencias de dispersión utilizadas en CDMA?

PROBLEMAS

1. ¿Es posible utilizar los valores 1 0 0… 0, 0 1 0 0…0, 0 0 1 0….0,00010…0, y así sucesivamente, como secuencias de dispersión de los nodos de una red que soporta CDMA basada en DSSS?
2. Sugiera una secuencia de dispersión de 11 bits diferente de la de Barker y mencione la posibilidad de detectar de manera confiable el comienzo de la transmisión del siguiente bit de la información fuente.

11

REDES DE TRANSMISIÓN

DESCRIPCIÓN DEL CAPÍTULO

11.1 INTRODUCCIÓN

Las **redes de transmisión** están diseñadas para construir una infraestructura conmutada utilizando lo que sea posible para administrar de manera rápida y flexible un canal permanente "punto a punto" entre los dos dispositivos de los usuarios terminales. Las redes de transmisión emplean la técnica de conmutación de circuitos, mientras que las redes superpuestas, como las telefónicas y las de computadoras, operan con base en circuitos formados por redes de transmisión. Los canales que tales redes proporcionan a sus suscriptores se distinguen por un elevado ancho de banda: generalmente en el rango de 2 Mbps a 10 Gbps.

Existen tres generaciones de redes de transmisión:

- Jerarquía digital presíncrona (PDH)
- Jerarquía digital síncrona (SDH) (en Estados Unidos, el estándar SONET corresponde a la tecnología SDH)
- Multiplexaje por división de onda densa (DWDM)

Las primeras dos tecnologías —PDH y SDH— utilizan el multiplexaje por división de tiempo para compartir un enlace de banda ancha y transmitir datos en forma digital. Cada una de esas tecnologías soporta una jerarquía de velocidad de transmisión, por lo que el usuario puede seleccionar la velocidad deseada para los canales con base en la cual se construirá la red superpuesta.

La tecnología SDH garantiza velocidades mayores que la jerarquía PDH; por lo tanto, cuando se construye una red de transmisión de gran tamaño, su troncal generalmente se basa en la tecnología SDH y la red de acceso emplea la tecnología PDH.

Las redes DWDM representan el último logro en la creación de canales de comunicaciones rápidos. No son digitales pues proporcionan a sus usuarios una onda independiente para la transmisión de información. Los usuarios son libres de usar esta onda como quieran, implementando ya sea modulación o codificación. En la actualidad, la tecnología DWDM obliga a la tecnología SDH a salir de las troncales de larga distancia hacia la periferia de la red, con lo cual se convierte a SDH en una tecnología de red de acceso.

Existen tres tecnologías de conmutación y multiplexaje que permiten crear una red de transmisión flexible y escalable capaz de brindar servicio a un gran número de redes telefónicas y de computadoras.

11.2 REDES PDH

PALABRAS CLAVE: red de transmisión, jerarquía digital presíncrona (PDH), jerarquía digital síncrona (SDH), SONET, multiplexaje por división de onda densa (DWDM), jerarquía de velocidades, sistemas portadores T, sistemas portadores E, multiplexor T-1, protocolo de señalización, robo de bits, nivel de señal digital n, canal T-1/E-1 fraccional, operaciones de multiplexaje/demultiplexaje y acarreo hacia atrás.

La **jerarquía digital presíncrona** (PDH) fue diseñada a finales de la década de 1960 por AT&T para resolver el problema de interconexión de switches en grandes redes telefónicas. Los canales FDM que se habían utilizado para resolver este problema ya habían agotado todas sus posibilidades de administrar las comunicaciones multicanal de alta velocidad a través de un solo cable. Con el fin de mejorar la velocidad de las comunicaciones, fue necesario instalar cables con muchos pares o reemplazarlos por cables coaxiales muy costosos.

11.2.1 Jerarquía de velocidades

El punto de partida de la evolución de la tecnología PDH fue el diseño del multiplexor T-1, el cual podía multiplexar, conmutar y transmitir en forma digital (continua) el tráfico de voz proveniente de 24 abonados. Como los abonados continuaron utilizando aparatos telefónicos estándar, lo cual significaba que la transmisión de la voz se llevaba a cabo de manera analógica, el T-1 multiplexaba automáticamente voces a una velocidad de 8 000 Hz y la codificaba mediante una modulación por pulsos codificados. En consecuencia, cada loop local formaba un flujo de datos digitales de 64 Kbps y toda la línea T-1 garantizaba un ancho de banda de 1 544 Mbps.

Los enlaces T-1 no eran herramientas de multiplexaje lo suficientemente flexibles y poderosas para conectar grandes centrales automáticas. Por lo tanto, se ideó formar enlaces de comunicaciones con una **velocidad jerárquica**. Se juntaron *cuatro* enlaces: T-1 para integrar los enlaces del siguiente nivel de la jerarquía digital, T-2, que transmitían datos a una velocidad de 6 312 Mbps. El enlace T-3 formado al unir siete enlaces y T-2 tiene una velocidad de 44 736 Mbps, mientras que el enlace T-4 une seis enlaces T-3; como resultado, su velocidad es de 27 4176 Mbps. Esta tecnología se conoce con el nombre de **sistemas portadores T**.

A mediados de la década de 1970, las compañías telefónicas comenzaron a proporcionar enlaces dedicados construidos con base en sistemas de portadores T para su arrendamiento comercial y dejaron de ser una tecnología interna de dichas compañías. Los enlaces T-1 a T-4 permitían retransmitir no sólo voz, sino también cualquier otro tipo de datos representados de manera digital, como los de computadora, televisión y fax.

La tecnología de sistemas portadores T fue estandarizada por el Instituto Nacional de Estándares Americanos (ANSI) y después por el CCITT, actualmente conocido como el ITU-T. Después de la estandarización, se conoció como PDH. Como resultado de las modificaciones realizadas por el CCITT, las versiones estadounidense e internacional del estándar PDH fueron incompatibles. En el estándar internacional, los enlaces análogos a los T son los E-1, E-2, E-3 y E-4, los cuales difieren en las velocidades de 2 048, 8 488, 34 368 y 13 9264 Mbps, respectivamente. La versión estadounidense del estándar también fue adoptada en Canadá y Japón (con sólo unas pequeñas diferencias); a su vez, en Europa se utiliza el estándar internacional del CCITT.

A pesar de las diferencias en las versiones estadounidense e internacional del estándar, las tecnologías de la jerarquía digital usan la misma notación para designar la jerarquía de velocidades: **nivel de señal digital n** (DS-n). La tabla 11.1 constituye una lista con los valores de todos los niveles de velocidades de datos incluidos en los estándares de ambas tecnologías.

11.2.2 Métodos de multiplexaje

El multiplexor T-1 garantiza la transmisión de datos de 24 abonados a 1 544 Mbps en una trama que tiene un formato simple. En esta trama, los datos del usuario se transmiten de manera secuencial: 1 byte de cada abonado a la vez y, después de 24 bytes, se agrega un *bit de sincronización*. Inicialmente, los dispositivos T-1 (los cuales dan nombre a toda la tecnología de transmisión de datos a 1 544 Mbps) operaban sólo con un reloj interno y cada trama podía transmitirse de manera asíncrona mediante bits de sincronización. Los dispositivos T-1, así como el equipo más rápido T-2 y T-3 han experimentado cambios significativos durante sus largos años de existencia. En la actualidad, los multiplexores y switches de la red de transmisión trabajan con la frecuencia de un reloj centralizado desde un solo punto en la red. Sin embargo, el principio de tramado sigue siendo el mismo; por lo tanto, los bits de

TABLA 11.1 Jerarquía de velocidades de datos digitales

América				CCIT (Europa)		
Designación de la velocidad	Número de canales de voz	Número de canales del nivel jerárquico anterior	Velocidad en Mbps, a menos que especifique otra cosa	Número de canales de voz	Número de canales del nivel jerárquico anterior	Velocidad en Mbps, a menos que especifique otra cosa
DS-0	1	1	64 kbps	1	1	64 kbps
DS-1	24	24	1 544	30	30	2 048
DS-2	96	7	6 312	120	4	8 488
DS-3	672	7	44 736	480	4	34 368
DS-4	4 032	6	274 176	1 920	4	139 264

En la práctica, los enlaces T-1/E-1 y T-3/E-3 se utilizan muy ampliamente.

sincronización aún están presentes en la trama. La velocidad total de los canales del usuario es de 24 abonados × 64 Kbps = 1.536 Mbps y se agregan 8 Kbps como bits de sincronización, lo cual da una suma total de 1.544 Mbps.

Ahora considere otra característica del formato de la trama T-1. En el equipo T-1, el octavo bit *de cada byte* de la trama tiene un significado especial en función del tipo de datos que se transmiten y de la generación del equipo. Cuando se transmite voz, este bit se utiliza para información de servicio, por ejemplo: el número del abonado llamado y otra información necesaria para establecer una conexión entre los abonados de la red. El protocolo que garantiza dicha conexión en telefonía se conoce como **protocolo de señalización**. Por ende, la velocidad real de la transmisión de voz del usuario es de 56 Kbps en lugar de 64 Kbps. La técnica que consiste en emplear el octavo bit para propósitos de servicio se llama **robo de bits**.

Cuando sólo se transmiten datos de computadora, la línea T-1 brinda 23 canales de datos del usuario y el canal 24 se utiliza exclusivamente para uso interno, en especial para restablecer tramas dañadas. Los datos de computadora se transmiten a 64 Kbps, pues el octavo bit no es "robado".

Durante la transmisión simultánea de datos de voz y de computadora se usan los 24 canales y ambos se transmiten a 56 Kbps.

Cuando se multiplexan cuatro canales T-1 en un solo canal T-2, se utiliza un bit de sincronización entre las tramas DS-1 como se hizo antes y las tramas DS-2 (las cuales contienen cuatro tramas DS-1 secuenciales) están separadas por 12 bits de servicio, los cuales se usan no sólo para separar las tramas, sino también para sincronizarlas. De acuerdo con esto, las tramas DS-3 comprenden siete tramas DS-2 separadas por bits de servicio.

Como se mencionó antes, la versión de la tecnología PDH descrita en los estándares internacionales G.700-G.706 del CCITT difiere respecto a la tecnología de sistemas portadores T estadounidenses. En particular, no emplea el método de robo de bits. Cuando se va

al siguiente nivel de la jerarquía, el multiplicador de velocidades tiene un valor constante de 4. En lugar del octavo bit, la línea E-1 asigna, para efectos de servicio, dos de los 32 bytes, los cuales son el byte 0 (para sincronizar entre el transmisor y el receptor) y el byte 16 (para transmitir información de señalización). Para la transmisión de voz o datos existen 30 canales disponibles, cada uno de los cuales tiene una velocidad de 64 Kbps.

El usuario puede arrendar varios canales de 56/64 Kbps del enlace T-1/E-1. Dicho canal compuesto se conoce como T-1/E-1 *fraccional*. En este caso, al usuario se le asignan varias ranuras de tiempo en el multiplexor.

La capa física de la tecnología PDH soporta varios tipos de cable: par trenzado, coaxial y fibra óptica. La variante principal de la administración del acceso de abonado a los enlaces T-1/E-1 es un cable que consiste en dos pares trenzados con conectores RJ-48. Para administrar el modo dúplex de la transmisión de datos a una velocidad de 1.544/2.048 Mbps son necesarios dos pares. Los canales T-1 utilizan el código potencial bipolar B8ZS para representar datos, mientras que los canales E-1 usan el código potencial bipolar HDB3 para el mismo propósito. Para amplificar señales en las líneas T-1, se instalan regeneradores y equipo con el fin de controlar la línea después de cada 1 800 metros (1 milla).

El cable coaxial, debido a su gran ancho de banda, soporta un canal T-2/E-2 o cuatro canales T-1/E-1. En los canales T-3/E-3 se utiliza el cable coaxial, la fibra óptica o las microondas.

La capa física de la variante internacional de esta tecnología se describe en el estándar G.703, cuyo nombre designa el tipo de interfaz de puente o ruteador conectado al canal E-1. La versión estadounidense del estándar se llama T-1.

11.2.3 Limitaciones de la tecnología PDH

Tanto la versión estadounidense como la internacional del estándar tecnológico PDH tienen varias limitaciones, entre las cuales las más importantes son la complejidad y la *ineficiencia de las operaciones de multiplexaje/demultiplexaje* de los datos del usuario. El término en sí mismo —*presíncrono* (es decir, casi síncrono)— utilizado para nombrar esta tecnología es una evidencia implícita de la falta de sincronización total cuando se multiplexan canales de baja velocidad en canales de velocidad más alta. En un principio, el método asíncrono de la transmisión de tramas hace que sea necesario insertar bits de sincronización entre las tramas.

Como resultado, para recuperar los datos del usuario a partir de un canal multiplexado es necesario demultiplexar **totalmente** las tramas a partir del canal agregado. Por ejemplo, para recuperar los datos del canal de un abonado específico de 64 Kbps a partir de las tramas del canal T-3, se deben demultiplexar estas tramas a nivel de la trama T-2, continuar con esta operación hasta el nivel de la trama T-1 y, por último, demultiplexar las tramas T-1.

Si se utiliza la red PDH como una troncal sólo entre dos nodos grandes, las operaciones de multiplexaje/demultiplexaje se llevarán a cabo únicamente en los nodos terminales; en consecuencia, no se presentará ningún problema. Sin embargo, cuando se requiere derivar uno o más canales de abonado en un nodo de tránsito de la red PDH, la solución se torna un poco compleja. Un método posible para llevar a cabo esta tarea consiste en instalar dos multiplexores T3/E3 (o de más alto nivel) en cada nodo de la red (figura 11.1). El primer multiplexor lleva a cabo la demultiplexación total del flujo y envía parte de los canales lentos a los abonados; el segundo dispositivo multiplexa de nuevo el flujo de salida de alta velocidad de los canales que quedan. Cuando se implementa esta técnica, el número de dispositivos en operación se duplica.

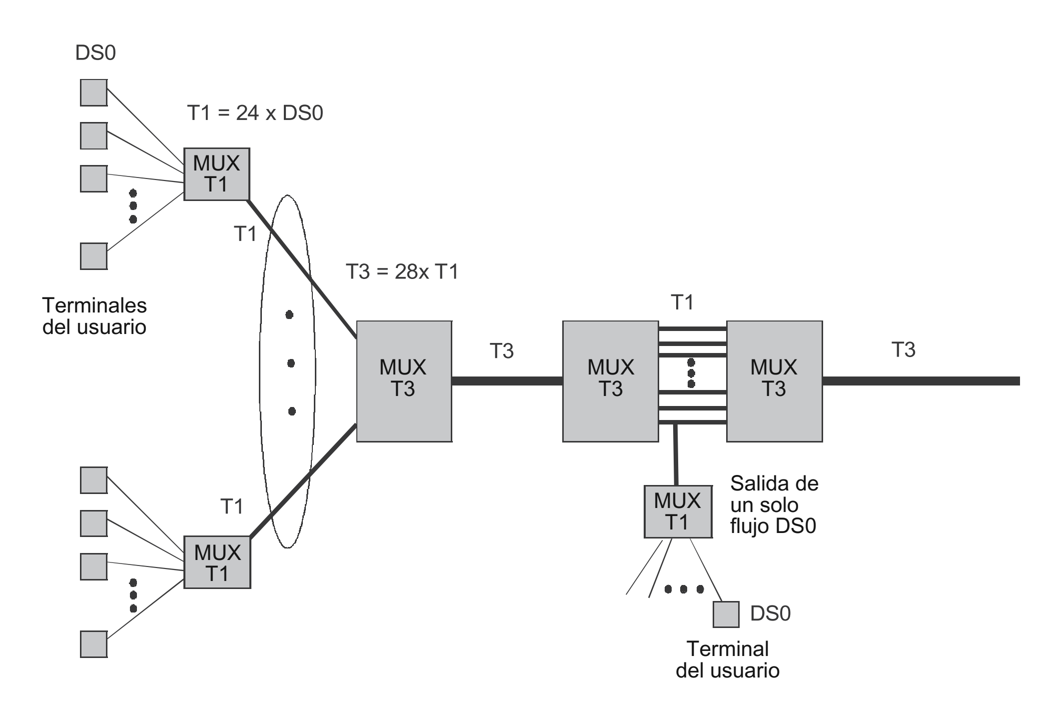


FIGURA 11.1 Separación de un canal de baja velocidad con el uso del demultiplexaje completo.

Otra variante es el **acarreo hacia atrás**. En el nodo de tránsito, donde es necesario separar y reenviar el flujo de abonado, se instala sólo el demultiplexor de alta velocidad, el cual simplemente transfiere los datos a una distancia más lejana de la red sin demultiplexarlos. Esta tarea es llevada a cabo por el demultiplexor de nodo terminal luego de que los datos destinados a un abonado específico regresan al nodo de tránsito a través de un enlace físico independiente. Como es natural, dicha operación compleja entre switches dificulta el funcionamiento manual de toda la red y requiere que esta última se tenga que configurar. Esto incrementa la cantidad de operaciones requeridas para la configuración manual de la red y, por lo tanto, puede causar errores.

Asimismo, la tecnología PDH no brinda herramientas incluidas para administrar la red ni para tolerar fallas.

Por último, PDH garantiza velocidades de transmisión de datos muy lentas de acuerdo con los requerimientos actuales. Los cables de fibra óptica permiten transmitir datos a velocidades de varios gigabits por segundo a través de una sola fibra, lo cual facilita el multiplexaje de decenas de miles de canales de abonado dentro de un solo cable. Sin embargo, la tecnología PDH no emplea esta característica, ya que su jerarquía de velocidades está limitada a 139 Mbps.

11.3 REDES SONET/SDH

PALABRAS CLAVE: módulo de nivel N para el transporte síncrono (STM-N), señal de transporte síncrono nivel N (STS-N), portador óptico nivel N (OC-N), contenedor virtual, tabla de conexiones, tabla de conexión cruzada, apuntador, unidad tributaria, unidad administrativa, multiplexor SDH, multiplexor terminal, multiplexor agregar/quitar, puerto de un tributario,

puertos agregar/quitar, puerto agregado, puerto de línea, regenerador, pila de protocolos SDH, sección del regenerador, información adicional de la sección del regenerador, sección del multiplexor, información adicional de la sección del multiplexor, alineación positiva, alineación negativa, topología de la red SDH, anillo SDH, secuencia lineal de multiplexores, tolerancia a fallas, conmutación con protección automática, red autorreconfigurable, conmutación para proteger el equipo (EPS), protección de tarjetas, protección de la sección del multiplexor (MSP), protección de la conexión de la subred (SNC-P) y anillo con protección compartida de la sección del multiplexor (MS-SPRing).

Las limitaciones mencionadas acerca de la tecnología PDH fueron tomadas en cuenta y eliminadas por los diseñadores de la tecnología de la **red óptica síncrona (SONET)**. La primera versión de este estándar apareció en 1984. Después de eso, dicha tecnología fue estandarizada por el comité T-1 de la ANSI. La estandarización internacional de esta tecnología se llevó a cabo con la coordinación del Instituto Europeo para la Estandarización de las Telecomunicaciones (ETSI) y la ITU-T en cooperación con la ANSI y varias compañías líderes en telecomunicaciones de América, Europa y Japón. El objetivo principal de los diseñadores del estándar internacional fue crear tecnología capaz de transmitir el tráfico de todos los canales digitales existentes del nivel PDH (tanto los T1-T3 estadounidenses como los E1-E4 europeos) mediante el uso de una troncal de alta velocidad basada en cables de fibra óptica, así como garantizar una jerarquía de velocidades que fuera una continuación de la jerarquía PDH a velocidades de varios gigabits por segundo.

Como consecuencia de un prolongado esfuerzo de cooperación, el ITU-T y el ETSI diseñaron el estándar internacional conocido como **jerarquía digital síncrona (SDH)**. El estándar SONET también fue elaborado para garantizar la compatibilidad del equipo. Por lo tanto, las redes SDH y SONET son compatibles (pero no idénticas) y pueden multiplexar flujos de entrada de prácticamente cualquier estándar PDH: europeo o estadounidense.

11.3.1 Jerarquía de velocidades y métodos de multiplexaje

La jerarquía de velocidades soportada por las tecnologías SONET/SDH se muestra en la tabla 11.2.

En el estándar SDH, todos los niveles de velocidad (y, por consiguiente, los formatos de trama de dichos niveles) tienen el mismo nombre: **módulo de transporte síncrono de nivel N (STM-N)**. En la tecnología SONET existen dos designaciones para los niveles de velocidad: **señal de transporte síncrono de nivel N (STS-N)**, utilizado para transmitir datos mediante señales eléctricas y el **portador óptico de nivel N (OC-N)**, empleado cuando se transmiten datos a través del cable de fibra óptica. Además, para efectos de simplicidad, el análisis se centrará en la tecnología SDH.

Las tramas STM-N tienen una estructura compleja que permite añadir flujos SDH y PDH a diferentes velocidades al flujo principal común y el desempeño de las operaciones de adicionar/remover sin demultiplexar totalmente el flujo principal.

Las operaciones de multiplexaje y de adicionar/quitar utilizan **contenedores virtuales** en los que los bloques de datos PDH pueden transportarse a través de la red SDH. Además de los bloques de datos PDH, se coloca información de control auxiliar en los contenedores virtuales, incluido el encabezado de la información de relleno de la trayectoria del contenedor. Este encabezado contiene información estadística acerca del proceso de envío del contenedor por su ruta desde el origen hasta el destino (mensajes de error), así como datos de control como un indicador del establecimiento de la conexión entre los puntos terminales. Como

TABLA 11.2 Jerarquía de velocidades SONET/SDH

SDH	SONET	Velocidad
	STS-1, OC-1	51.84 Mbps
STM-1	STS-3, OC-3	155.520 Mbps
STM-3	OC-9	466.560 Mbps
STM-4	OC-12	622.080 Mbps
STM-6	OC-18	933.120 Mbps
STM-8	OC-24	1.244 Gbps
STM-12	OC-36	1.866 Gbps
STM-16	OC-48	2.488 Gbps
STM-64	OC-192	9.953 Gbps
STM-256	OC-768	39.81 Gbps

resultado, el tamaño del contenedor virtual es más grande que la correspondiente carga útil PDH que lleva. Por ejemplo, el VC-12, además de los 32 bytes de datos del flujo E-1, contiene 3 bytes de información de control. En la tecnología SDH, existen varios tipos de contenedores virtuales (figura 11.2) para transportar los principales tipos de bloques de datos PDH: VC-11 (1.5 Mbps), VC-12 (2 Mbps), VC-2 (6 Mbps), VC-3 (34/45 Mbps) y VC-4 (140 Mbps).

Los contenedores virtuales son *unidades de conmutación* de multiplexores SDH. En cada multiplexor existe una **tabla de conexión** (también llamada **tabla de conexión cruzada**) que especifica, por ejemplo, que el VC-12 del puerto P1 está conectado al VC-12 del puerto P5 y que el VC-3 del puerto P8 se halla conectado al VC-3 del puerto P9. El administrador de la red construye la tabla de conexiones en cada multiplexor mediante un sistema de administración o una terminal de control. Esta operación debe realizarse de tal forma que asegure la trayectoria que conecta los dos nodos terminales de la red a los que el equipo del usuario está conectado.

Para combinar la transmisión síncrona de las tramas STM-N con la naturaleza asíncrona de los datos del usuario PDH transportados por estas tramas dentro de la misma red, la tecnología SDH utiliza **apuntadores**. El concepto de apuntadores es la clave de la tecnología SDH, la cual reemplaza la ecualización de la velocidad de las fuentes asíncronas con bits redundantes, misma que fue adoptada en PDH.

El apuntador determina la posición actual de un contenedor virtual en la capa más alta de la estructura: una **unidad tributaria** o una **unidad administrativa**. La diferencia principal entre estas unidades respecto a los contenedores virtuales es la presencia de un campo apuntador adicional. Debido al uso de apuntadores, un contenedor virtual puede "flotar" dentro de ciertos límites en su unidad tributaria o administrativa. Ésta, en contraste, tiene una posición fija dentro de una trama. Debido al sistema de apuntadores, el multiplexor puede encontrar la posición de los datos de los usuarios en el flujo de bytes síncrono de las tramas STM-N y recuperarlas "en caliente". Observe que el mecanismo de multiplexaje implementado en PDH no ofrece esta facilidad.

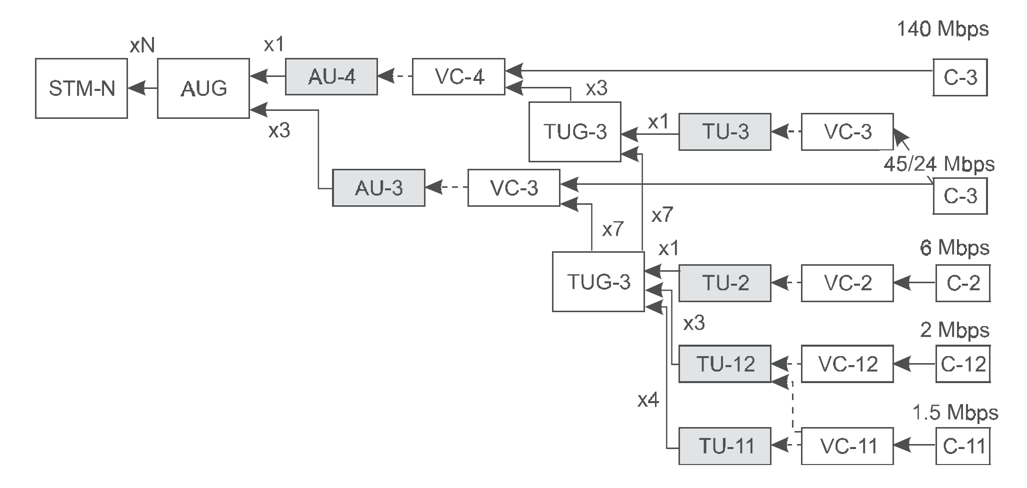


FIGURA 11.2 Método del multiplexado de datos en SDH.

Las unidades tributarias se unen en grupos, que a su vez se agrupan en unidades administrativas. El grupo de *N* unidades administrativas conforma la carga útil de la trama STM-N. Además, la trama cuenta con un encabezado que contiene información de control, la cual es común a todas las unidades administrativas. En cada etapa de transformación de los datos del usuario se agregan varios bytes de control a los datos de la fuente. Estos bytes auxiliares ayudan a reconocer la estructura del bloque o grupo de bloques y después, mediante el uso de apuntadores, determinan el punto donde comienzan los datos del usuario.

La figura 11.2 muestra las unidades estructurales de la trama SDH. Las unidades que contienen los apuntadores están bloqueadas y la relación entre los contenedores y unidades, que permiten correr en fase los datos, se señala con línea punteada.

El método de multiplexaje SDH proporciona diferentes facilidades para agregar flujos de usuarios PDH. Por ejemplo, en la trama STM-1 se pueden implementar las variantes siguientes:

- 1 ráfaga E-4
- 63 ráfagas E-1
- 1 ráfaga E-3 y 42 ráfagas E-1

Ciertamente, usted puede sugerir otras variantes.

11.3.2 Tipos de equipos

El elemento principal de la red SDH es el **multiplexor** (figura 11.3). En general, éste se encuentra equipado con cierto número de puertos PDH y SDH, por ejemplo: puertos PDH a 2 Mbps y 34/45 Mbps, puertos STM-1 diseñados a 155 Mbps y puertos STM-4 diseñados a 622 Mbps. Los puertos del multiplexor SDH se clasifican en agregados y tributarios. Los *puertos tributarios* a menudo se llaman *puertos de agregar/remover* y los *puertos agregados* se denominan *puertos de línea.* Esta terminología refleja las topologías típicas de las redes SDH, donde existe una troncal pronunciada (línea) en forma de una cadena o anillo a través del cual las ráfagas de datos provenientes de los usuarios de la red se transmiten mediante los puertos agregar/remover.

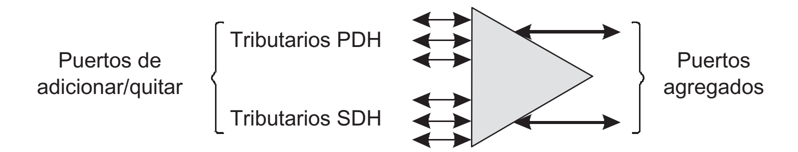


FIGURA 11.3 Multiplexor SDH.

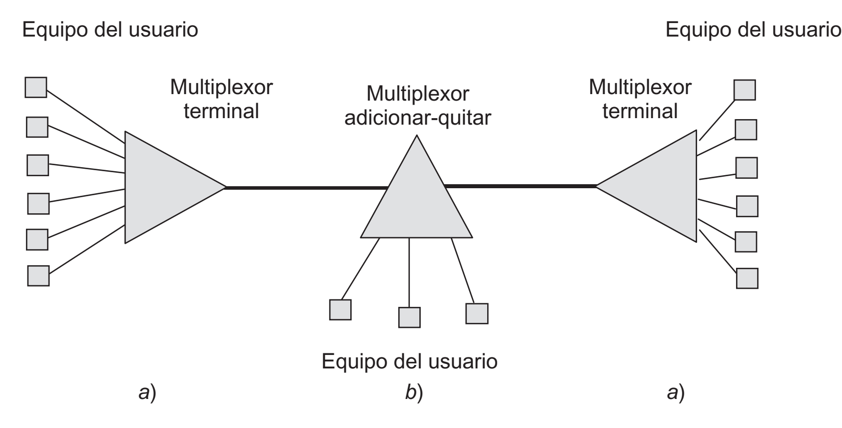


FIGURA 11.4 Tipos de multiplexores SDH.

Los multiplexores SDH se dividen, por lo general, en dos tipos y la diferencia entre ellos depende de la posición del multiplexor en la red SDH:

- **Multiplexores terminales.** Son aquellos que finalizan los canales agregados al multiplexar un gran número de canales tributarios (figura 11.4*a*). Por lo tanto, el multiplexor terminal está equipado con un puerto agregado y muchos puertos tributarios.
- **Multiplexores agregar/remover**. Se encuentran ubicados en una posición intermedia en la troncal (anillo, cadena o topología híbrida). Cuentan con dos puertos agregados para transmitir la ráfaga de datos agregada (figura 11.4*b*). Mediante el uso de un reducido número de puertos tributarios, dicho multiplexor agrega o quita los datos de los canales tributarios a/o de la ráfaga agregada.

A veces existen **conexiones cruzadas digitales**: multiplexores que llevan a cabo operaciones de conmutación en contenedores virtuales arbitrarios. En dichos multiplexores no hay diferencias entre los puertos agregados y tributarios, pues dicho multiplexor está diseñado para trabajar en topología de malla, donde es imposible distinguir las ráfagas agregadas.

Además de multiplexores, la red SDH puede contar con los **regeneradores** necesarios para eliminar las limitaciones en cuanto a la distancia entre multiplexores. Dichas limitaciones dependen de la potencia de los transmisores ópticos, la sensibilidad de los receptores y la atenuación de cable de fibra óptica (este problema se planteó en el *capítulo 8* como un ejercicio acerca de presupuesto de potencia*)*. El regenerador transforma la señal óptica en una señal eléctrica y después otra vez en una señal óptica. En el transcurso de esta operación, tanto las características de la forma de la señal como su temporización se restablecen. Hoy en día, los regeneradores SDH se utilizan muy rara vez, ya que su costo no es mucho menor que el del multiplexor y sus características de funcionalidad no se pueden comparar con las de éstos.

11.3.3 Pila de protocolos

La **pila de protocolos SDH** está formada por cuatro capas, las cuales no se relacionan con las del modelo OSI. Desde el punto de vista del modelo OSI, la red SDH en su totalidad está constituida por equipo de la capa física.

- En la pila de protocolos SDH, la **capa fotónica** tiene que ver con la codificación de los bits de información mediante el uso de la modulación de la luz. Para codificar la señal óptica, se utiliza el código potencial NRZ. Esta propiedad de autosincronización del código se logra mediante la aleatorización de los datos antes de ser transmitidos.
- La **capa de sección** soporta la integridad física de la red. En términos de la tecnología SDH, una sección es cualquier porción continua de cable de fibra óptica que conecta un par de dispositivos SONET/SDH (por ejemplo, puede conectar un multiplexor con un regenerador o un regenerador con otro regenerador). La sección se llama a menudo **sección del regenerador**, suponiendo que para que esta capa realice sus funciones no se requiere que los dispositivos terminales de la sección sean multiplexados. El protocolo de la sección del regenerador tiene que ver con una parte específica del encabezado de la trama, conocida como **información de relleno de la sección del regenerador**. Con base en la información de control, este protocolo puede probar la sección y soportar funciones de control administrativo.
- La **capa lineal** es responsable de transmitir datos entre dos multiplexores de red. El protocolo de esta capa se relaciona con las tramas de la capa STS-N para el multiplexaje y demultiplexaje, así como la adición y remoción de los datos del usuario. Al protocolo lineal también se atribuye la reconfiguración de la línea si falla uno de sus elementos, ya sea la fibra óptica, un puerto o un multiplexor adyacente. Con frecuencia, la línea se llama **sección del multiplexor**. La información de control de la sección del multiplexor se coloca dentro de la parte del encabezado de la trama, llamada **información de relleno de la sección del multiplexor** (MSOH).
- La **capa de trayectoria** es responsable de la entrega de los datos entre dos usuarios de la red. La trayectoria es una conexión virtual compuesta entre usuarios. El protocolo de la capa de trayectoria debe recibir los datos que se proporcionan en el formato del usuario (por ejemplo, en el formato T-1) y transformarlos en tramas síncronas STM-N.

La figura 11.5 muestra la distribución de los protocolos SDH por tipo de equipo SDH.

11.3.4 Tramas STM-N

Los elementos principales de la trama STM-1 se muestran en la figura 11.6 y la tabla 11.3 describe la estructura de los encabezados de las secciones del regenerador y del multiplexor. En general, la trama se representa como una matriz de 270 columnas y 9 renglones. Los primeros 9 bytes de cada renglón están reservados para los datos de servicio de los encabezados, mientras que 260 bytes de la secuencia de 261 bytes están dedicados a la carga útil (por ejemplo, los datos de estructuras, como las unidades administrativas, los grupos de unidades administrativas, las unidades tributarias, los grupos de unidades tributarios y los contenedores virtuales). Un byte de cada renglón está reservado para el encabezado de trayectoria, el cual permite controlar la conexión de un punto a otro.

Considere el mecanismo de la operación del apuntador H1-H2-H3 del ejemplo de la trama STM-1, el cual transporta el VC-4. El apuntador toma 9 bytes del cuarto renglón de la trama, cada uno de los cuales se toman de los campos H1, H2 y H3 a los que se les reservan

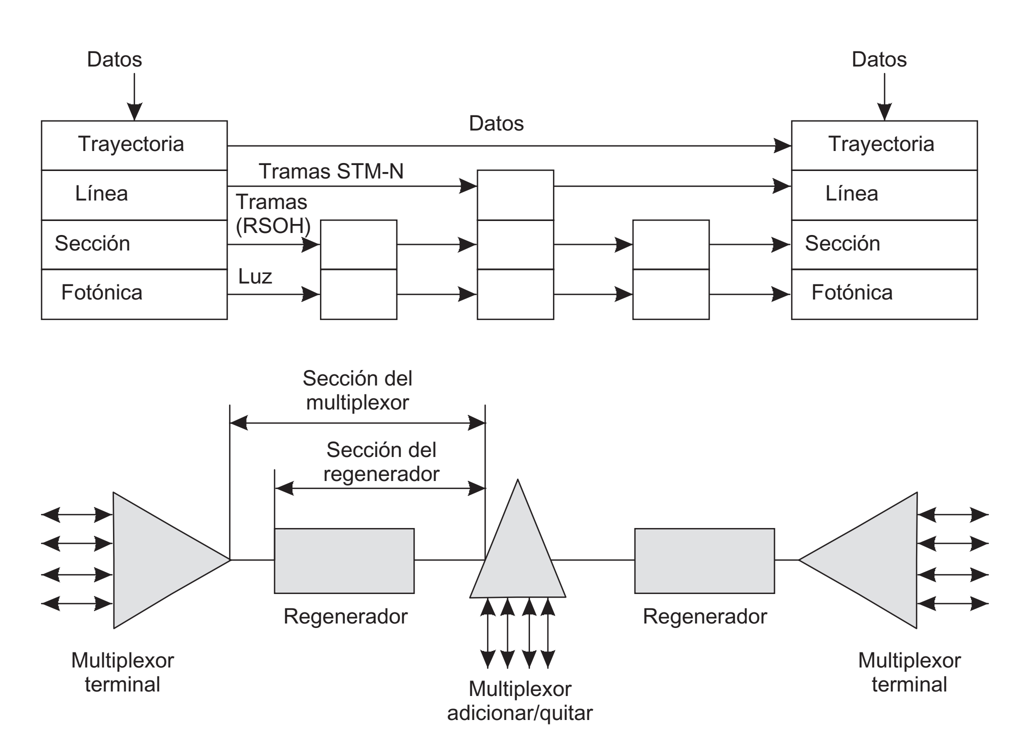


FIGURA 11.5 Pila de protocolos de la tecnología SDH.

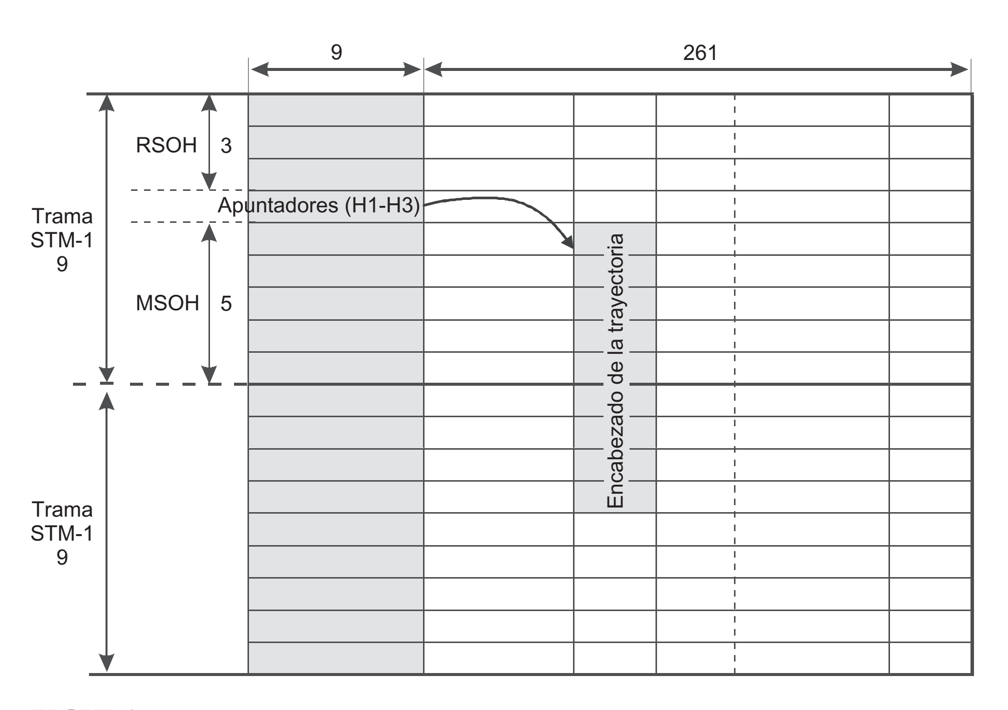


FIGURA 11.6 Estructura de la trama STM-1.

3 bytes. Los valores permitidos del apuntador pertenecen al rango de 0 a 782. El apuntador marca la posición de comienzo del VC-4 en unidades de 3 bytes. Por ejemplo, si el apuntador marca 27, el primer byte del VC-4 está ubicado en $27 \times 3 = 81$ bytes a partir del último

TABLA 11.3 Estructura de los encabezados de las secciones del regenerador y el multiplexor

Encabezado de la sección del regenerador	Encabezado de la sección del multiplexor
Bytes de sincronización	Bytes para el control de errores de la sección del multiplexor
Bytes para el control de errores de la sección del regenerador	6 bytes del DCC que funcionan a una velocidad de 576 Kbps
Un byte del canal de radio auxiliar (64 kbps)	2 bytes del protocolo de protección automática del tráfico (los bytes K1 y K2) que garantizan la supervivencia de la red
3 bytes del canal de comunicaciones (DCC) que trabaja a una velocidad de 192 Kbps	1 byte para los mensajes del estado del sistema de sincronización
Bytes reservados para usarlos a discreción por los prestadores de servicio nacionales	En los demás bytes, el encabezado MSOH está reservado para usarlo a discreción por los prestadores de servicios de comunicaciones nacionales o no se utilizan.
Los campos de los apuntadores H1, H2 y H3 especifican la posición del punto de comienzo del VC-4 o tres VC-3 en relación con el campo de los apuntadores.	

bit del campo del apuntador, lo cual significa que es el byte 90 (la numeración comienza en el 1) de la cuarta columna de la trama STM-1. El valor fijo del apuntador toma en cuenta el corrimiento de fase entre la fuente de datos (cuya función puede llevar a cabo el multiplexor PDH, el equipo del usuario terminal con la interfaz PDH/SDH u otro multiplexor SDH) y el multiplexor actual. Como resultado, el contenedor virtual se transmite en dos tramas STM-1 secuenciales, como se muestra en la figura 11.6.

El apuntador no sólo puede procesar corrimientos fijos de fase, sino también desajustes en la frecuencia del reloj entre el multiplexor y el dispositivo desde el cual se reciben los datos del usuario. Para compensar este efecto, el valor del apuntador se incrementa o disminuye de manera periódica en una unidad.

Si la velocidad de llegada de los datos de VC-4 es menor que la velocidad del STM-1 emisor, el multiplexor experimenta periódicamente (este periodo depende del valor de la desviación de la frecuencia de sincronización) una escasez de datos de usuario que son necesarios para llenar los campos apropiados del contenedor virtual. Por lo tanto, el multiplexor inserta tres bytes "de relleno" (insignificantes) en los datos del contenedor virtual, después de lo cual éste continúa llenando el VC-4 con los datos del usuario que llegaron durante la pausa. El apuntador se incrementa en una unidad, lo cual refleja el corrimiento del punto del comienzo del siguiente VC-4 en 3 bytes. Esta operación del apuntador se conoce como **alineación positiva**. Como resultado, la velocidad promedio de la transmisión de los datos del usuario es igual a la velocidad de su llegada sin insertar bits redundantes en la trama PDH.

Si la velocidad de llegada de los datos VC-4 es mayor que la velocidad del envío de la trama STM-1, el multiplexor periódicamente necesita insertar bytes "extra" en la trama (extra significa que no hay lugar en el campo VC-4 para estos bytes). Para colocar dichos bytes, se utilizan los tres bytes menos significativos del apuntador, esto es, el campo H3 (el valor del apuntador en sí mismo cabe dentro de los bytes de los campos H1 y H2). En este caso, el apuntador disminuye en uno; por lo tanto, dicha operación de conoce con el nombre de **alineación negativa**.

La razón de que la alineación de VC-4 se lleve a cabo en unidades de 3 bytes puede explicarse de manera sencilla. La trama STM-1 puede transportar un VC-4 o tres VC-3. Cada VC-3, en general, tiene tanto un valor de fase independiente en relación con el punto de comienzo de la trama como un valor de desviación de frecuencia. El apuntador VC-3, en contraste con el VC-4, comprende 3 bytes en lugar de 9: H1, H2 y H3 (cada uno de estos campos tiene una longitud de 1 byte). Estos tres apuntadores se colocan en los mismos bytes que el apuntador VC-4; sin embargo, se utiliza el método de entrelazado de bytes, de acuerdo con el cual los apuntadores están en el orden siguiente: H1-1, H1-2, H1-3, H2-1, H2-2, H2-3, H3-1, H3-2 y H3-3 (el segundo índice identifica el VC-3 específico). Los valores de los apuntadores VC-3 se interpretan en bytes en lugar de en unidades de 3 bytes. Cuando se logra el alineamiento negativo del VC-3, el byte extra se coloca en el byte adecuado—H3-1, H3-2 o H3-3— lo que depende del VC-3 sobre el cual se lleva a cabo esta operación.

Por lo tanto, es necesario explicar la selección del tamaño de la desviación de los VC-4. Dicho tamaño se seleccionó para unificar estas operaciones sobre los contenedores de cualquier tipo, colocados directamente en el grupo de la unidad administrativa de la trama STM-1. La alineación de los contenedores de la capa inferior siempre se realiza con un paso de 1 byte.

Cuando se unen los bloques de la unidad unitaria y la administrativa en grupos de acuerdo con el método descrito (consulte la figura 11.6), dichos bloques se entrelazan secuencialmente byte por byte, de tal forma que el periodo de la llegada de los datos del usuario en la trama STM-N coincide con el periodo de su llegada a puertos tributarios. Esto excluye la necesidad de almacenarlo de modo temporal; por lo tanto, es correcto decir que *SDH multiplexa los datos por transmitir en modo de tiempo real.*

11.3.5 Topologías típicas

En las redes SDH se utilizan varias topologías de enlaces. Las más frecuentes son anillos y cadenas lineales de multiplexores. La topología en malla, que es muy parecida a la conectada totalmente, también ha experimentado un área de aplicación creciente.

El **anillo SDH** está construido con base en multiplexores de agregar/quitar que tienen al menos dos puertos agregados (figura 11.7*a*). Los flujos de datos del usuario se agregan y se quitan del anillo al emplear puertos tributarios, con lo que se forman conexiones punto a punto (la figura muestra dos conexiones de este tipo). El anillo es una topología convencional que tiene la característica de ser tolerante a fallas: en condiciones de una ruptura en el cable o la falla de un multiplexor, la conexión permanecerá intacta, siempre y cuando esté dirigida a lo largo del anillo en la dirección contraria. Por lo general el anillo se construye con base en un cable con dos fibras ópticas. No obstante, a veces se utilizan los cables con cuatro fibras a fin de mejorar la confiabilidad y el ancho de banda.

La cadena (figura 11.7*b*) es una **secuencia lineal de multiplexores** en la que los dos multiplexores en los puntos terminales desempeñan el papel de terminales y los demás multiplexores son de agregar/quitar. En general, se utilizan las redes con topología en cadena

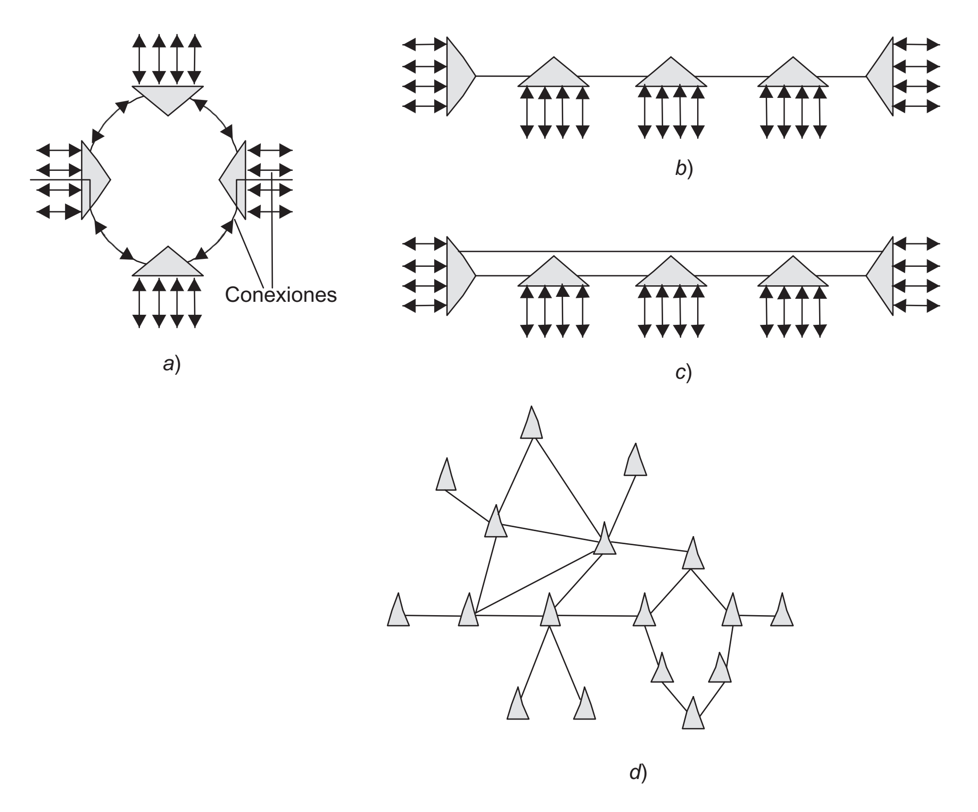


FIGURA 11.7 Topologías típicas.

cuando los nodos de la red tienen una ubicación geográfica específica, por ejemplo: cuando tienen que estar ubicados a lo largo de una vía de ferrocarril o en una línea de tubería. Sin embargo, en dichos casos también se puede usar el anillo plano (figura 11.7*c*), el cual garantiza un alto nivel de tolerancia a fallas mediante el uso de dos fibras adicionales en el cable troncal y la presencia de un puerto extra agregado en cada multiplexor terminal.

Dichas topologías base pueden combinarse a fin de construir una red SDH compleja y extensa con muchas ramas, con lo que se crean secciones con topología en anillo radial, conexiones de "anillo a anillo", etc. El caso más general es la topología en malla (figura 11.7*d*), en la cual los multiplexores se conectan entre sí mediante muchos enlaces que hacen posible lograr niveles muy altos de desempeño y confiabilidad.

11.3.6 Métodos para garantizar la supervivencia de la red

Uno de los aspectos más importantes de las redes de transmisión SDH es que cuenta con un gran número de herramientas que garantizan la tolerancia a fallas de la red. Tales herramientas permiten que la red se restablezca muy rápido (del orden de las decenas de milisegundos) después de presentarse una falla en algunos de sus elementos: ya sea un enlace de comunicaciones, un puerto o tarjeta del multiplexor o todo un multiplexor.

Los mecanismos de tolerancia a fallas de SDH se conocen con el término general de **conmutación automática de protección**, la cual refleja la conmutación a una trayectoria reservada o a un elemento multiplexor reservado en caso de una falla del elemento principal. Las redes que soportan dichos mecanismos se llaman **redes autorrecuperables** en los estándares de SDH.

En las redes SDH se utilizan los tres métodos de protección siguientes:

- La *protección 1+1* significa que un elemento redundante se encarga de llevar a cabo las mismas tareas que el elemento principal. Por ejemplo, cuando se protege la tarjeta de tributarios de acuerdo con el método 1+1, el tráfico pasa a través de la tarjeta principal (la que está trabajando) y de la tarjeta de respaldo (la redundante).
- La *protección 1:1* significa que el elemento redundante no realiza las funciones del elemento principal en el modo de operación normal, sino que sólo en caso de una falla en éste, el elemento redundante reemplazará sus funciones.
- La *protección 1:N* reserva un elemento redundante para *N* elementos que trabajan (es decir, los que necesiten protección). En caso de que falle uno de los elementos principales, el elemento redundante lo reemplazará y, por lo tanto, comenzará a llevar a cabo las funciones del elemento que falló. Si sucede esto, los demás elementos permanecerán sin protección alguna hasta que el elemento que falló sea reemplazado.

De acuerdo con el tipo de elemento que se proteja mediante la instalación de elementos redundantes, se utilizan cinco tipos principales de conmutación automática para proteger el equipo y las redes SDH.

El **equipo de conmutación para la protección (EPS)** protege unidades y elementos del equipo SDH y se utiliza en elementos de vital importancia del multiplexor, por ejemplo: la unidad de procesamiento, la unidad de conmutación (conexión cruzada), la unidad de alimentación y la unidad de entrada de señales de sincronización. Como regla general, el EPS opera de acuerdo con el método 1+1 o 1:1.

La **protección de tarjetas** se encarga de proteger las tarjetas tributarias y las de agregados del multiplexor. Permite que el multiplexor siga trabajando de modo automático en caso de una falla en una de las tarjetas agregadas o tributarias. En la protección de tarjetas se utilizan los tres métodos: 1+1, 1:1 y 1:N. La protección de acuerdo con el método 1+1 garantiza continuidad en el servicio de transporte, porque el tráfico que pasa a través de la conexión del usuario no se interrumpe en caso de que falle la tarjeta. La figura 11.8 propor-

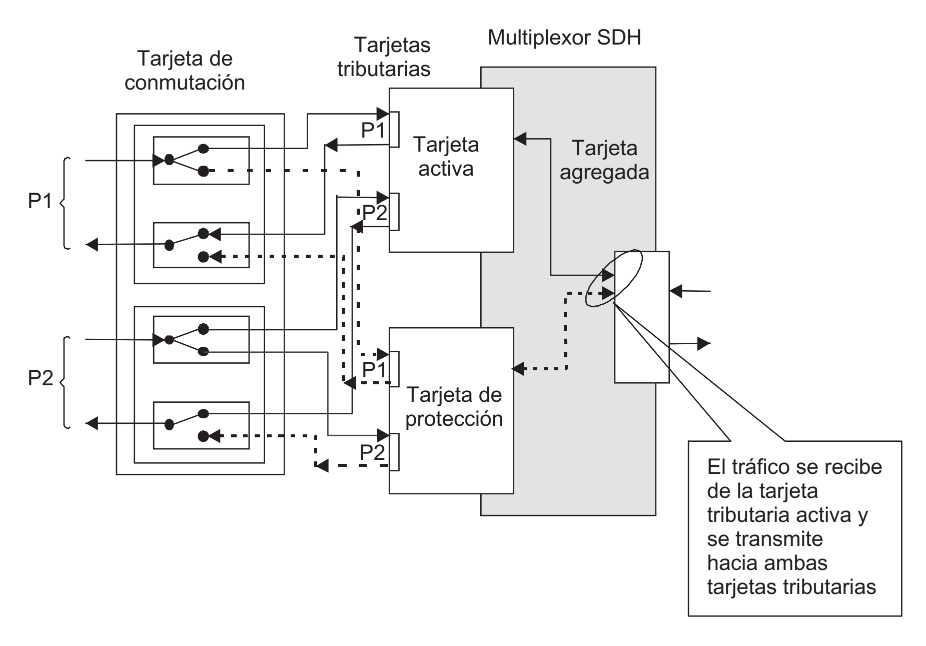


FIGURA 11.8 Protección de tarjetas de acuerdo con el método 1+1.

ciona un ejemplo de un multiplexor que soporta la protección de tarjetas con dos puertos tributarios de acuerdo con el método 1+1. Una de las tarjetas tributarias es la principal (la que trabaja) y la otra es la redundante (la de protección). El modo de operación del par de tarjetas conectadas de esta forma se determina mediante un comando especial utilizado en la configuración del multiplexor. Cuando ambas tarjetas tributarias están en operación, procesan el tráfico en paralelo.

Para conmutar tráfico entre tarjetas tributarias se utiliza una tarjeta de interruptor auxiliar. El tráfico entrante (adicional) que proviene de cada puerto alimenta al puente de entrada de la tarjeta del interruptor, la cual ramifica el tráfico y lo envía a las entradas de los puertos adecuados de las tarjetas tributarias. La tarjeta de agregados recibe ambas señales STM-N de las tarjetas tributarias y selecciona la señal de la tarjeta activa. El tráfico saliente (entregado) que viene de la tarjeta de agregados también es procesado por ambas tarjetas tributarias, pero solamente el tráfico de la tarjeta activa es enviado por el switch a su salida.

Cuando falla la tarjeta principal (o se presenta cualquier otro evento que requiera conmutación hacia la tarjeta de protección, como la degradación de la señal, errores en la señal, o remoción de la tarjeta), la tarjeta de agregados, mediante un comando de la unidad de control del multiplexor, conmuta para recibir la señal desde la tarjeta tributaria de protección. La tarjeta del interruptor, de manera simultánea, comienza a transmitir las señales del tráfico de bajada desde la tarjeta de protección hasta su salida.

Dicho método garantiza la protección automática de todas las conexiones que viajan a través de la tarjeta protegida. Cuando se especifica la protección de la tarjeta, la configuración de las conexiones de la tarjeta en modo de operación se duplica en la tarjeta de protección.

La **protección de la sección del multiplexor** (**MSP**) garantiza resguardar la sección del multiplexor (es decir, la sección de la red entre dos multiplexores SDH adyacentes). Actúa de manera más selectiva en comparación con la protección de la tarjeta. El objeto protegido es la sección entre dos multiplexores, incluidos dos puertos y el enlace de comunicaciones (el cual debe abarcar regeneradores pero no multiplexores). Como regla general se utiliza el método de protección 1+1. Cuando se emplea este método, se configura un enlace de protección (el par de puertos ubicados en la parte inferior) para el enlace activo (el par de puertos en la parte superior conectados por un cable), como se muestra en la figura 11.9*a*. Cuando

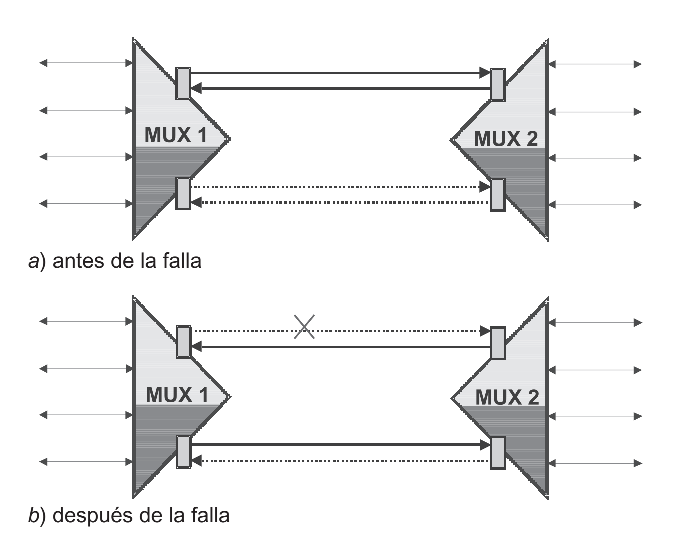


FIGURA 11.9 Protección de la sección de multiplexores (MSP).

se establece el MSP, es necesario configurar cada multiplexor especificando la relación entre el puerto activo y el de protección. En el estado inicial, todo el tráfico se transmite a través de los enlaces activos y de protección.

El MPS puede ser unidireccional o bidireccional. Cuando se utiliza protección unidireccional (la cual se muestra en la figura 11.9), solamente uno de los multiplexores (el de recepción en el caso del enlace que falla) decide si debe conmutar hacia el enlace de protección. Después de detectar la falla (falla en un puerto, error en la señal, degradación de la señal, etc.), este multiplexor conmuta para recibir la señal a través del enlace de protección. En este caso, tanto la transmisión como la recepción se llevan a cabo por medio de puertos diferentes (figura 11.9*b*).

Cuando se utiliza el MSP bidireccional, en el caso de una falla en el enlace activo en cualquier dirección, los multiplexores se conmutan a los puertos de protección. Para notificarle al multiplexor de transmisión (el cual usa el enlace activo) la necesidad de conmutar el enlace de protección, el multiplexor de recepción sigue un protocolo conocido con el nombre de *byte K*, el cual inserta el estado de los enlaces de protección y activos al proporcionar información detallada acerca de la falla, en 2 bytes del encabezado de la trama STM-N (los bytes K1 y K2 del MSOH). El mecanismo MSP garantiza la protección de todas las conexiones que pasan a través de la sección del multiplexor protegido. De acuerdo con los requerimientos del estándar, el tiempo de conmutación no debe exceder de 50 milisegundos.

La **protección de la conexión de la subred** (**SNC-P**) protege la trayectoria (conexión) a través de la red de un contenedor virtual específico. Dicho equipo asegura la conmutación de una conexión de usuario específica, hacia una trayectoria alterna en caso de que se presente una falla en la trayectoria principal. La tarea del SNC-P consiste en colocar el tráfico tributario en un tipo específico de contenedor virtual (por ejemplo, VC-12, VC-3 o VC-4). Se utiliza el método de protección 1+1.

El SNC-P se configura en dos multiplexores: el multiplexor de entrada, donde el tráfico tributario colocado en el contenedor virtual se ramifica, y el multiplexor de salida, donde se encuentran dos trayectorias alternas de tráfico. Un ejemplo de la implementación del SNC-P se muestra en la figura 11.10. En el multiplexor ADM1 se especifican dos conexiones para el VC-4 del puerto tributario T2: el de los cuatro VC-4 del puerto agregado A1 y el de los cuatro VC-4 del puerto agregados A2. Una de estas conexiones se configura como conexión activa; la otra es la conexión de protección. En el modo de operación normal, el tráfico se transmite a través de ambas conexiones. Los multiplexores de tránsito (para estas dos conexiones) se configuran de manera normal. En el multiplexor de salida ADM5, el VC-4 del puerto tributario T3 también está conectado a los contenedores: el del puerto agregado A1 y el del puerto agregado A2. Se selecciona el flujo de más alta calidad de los dos flujos que llegan al puerto T3. Si la calidad de ambos flujos es normal e igual, se seleccionará la señal proveniente del puerto agregado que está configurado como el puerto activo.

El SNC-P trabaja en las redes SDH con cualquier topología en la que existan rutas alternas de tráfico (es decir, con las topologías anillo y malla).

El **anillo de protección de la sección del multiplexor compartida** (**MS-SPRing**) es la protección de la trayectoria en la topología en anillo compartida entre las conexiones de usuario. En algunos casos, ésta garantiza la protección más eficaz del tráfico que circula por el anillo. A pesar de que el SNC-P es apropiado en la topología anillo de la red SDH, en algunos casos, su implementación reduce el ancho de banda efectivo del anillo debido a que cada conexión consume el doble de ancho de banda de todo el anillo. Por ejemplo, en el anillo STM-16 es posible establecer solamente 16 conexiones VC-4 protegidas de acuerdo con el método SNC-P (figura 11.11).

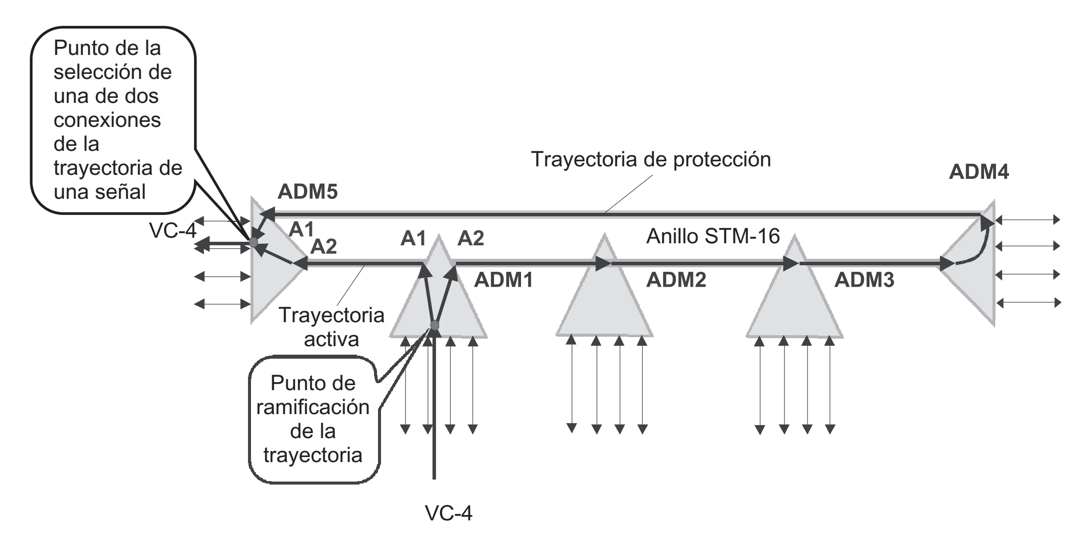


FIGURA 11.10 SNC-P.

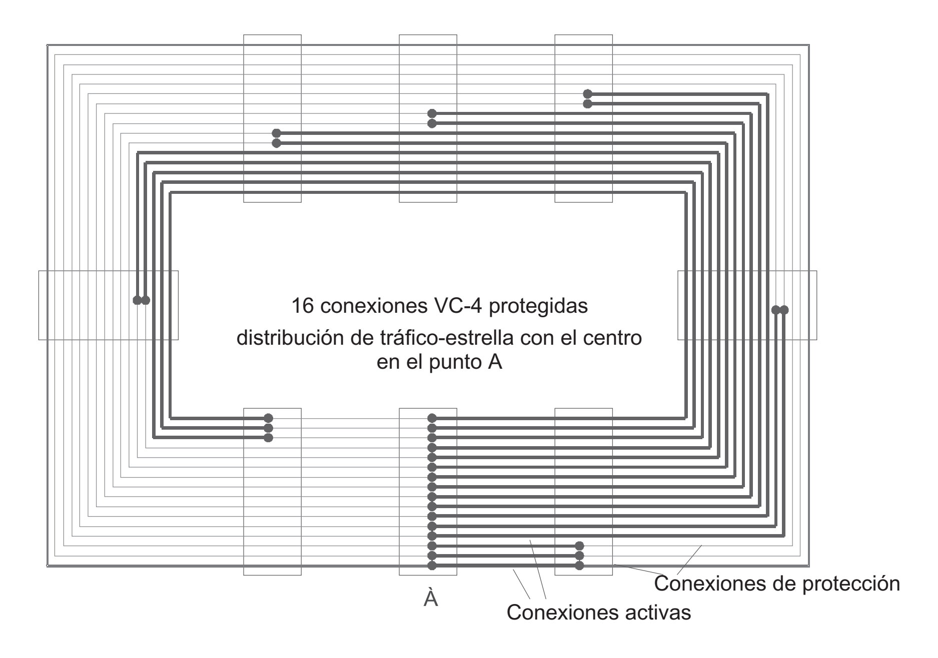


FIGURA 11.11 SNC-P en el anillo.

El MS-SPRing permite que el ancho de banda del anillo pueda ser utilizado de manera más eficiente debido a que el ancho de banda de cada conexión no es reservado con antelación. En lugar de esto, se reserva la mitad del ancho de banda del anillo, pero esto se hace de manera dinámica para conexiones conforme vaya siendo necesario (es decir, después de detectar una falla en un enlace o multiplexor). El nivel de ancho de banda disponible cuando se utiliza el MS-SPRing depende de la distribución del tráfico.

Si todo el tráfico proviene del mismo multiplexor (es decir, si se realiza una distribución en "estrella"), el MS-SPRing no proporcionará ningún ahorro económico comparado con el SNC-P. Un ejemplo de dicha situación se muestra en la figura 11.12*a*. En esta lámina, el

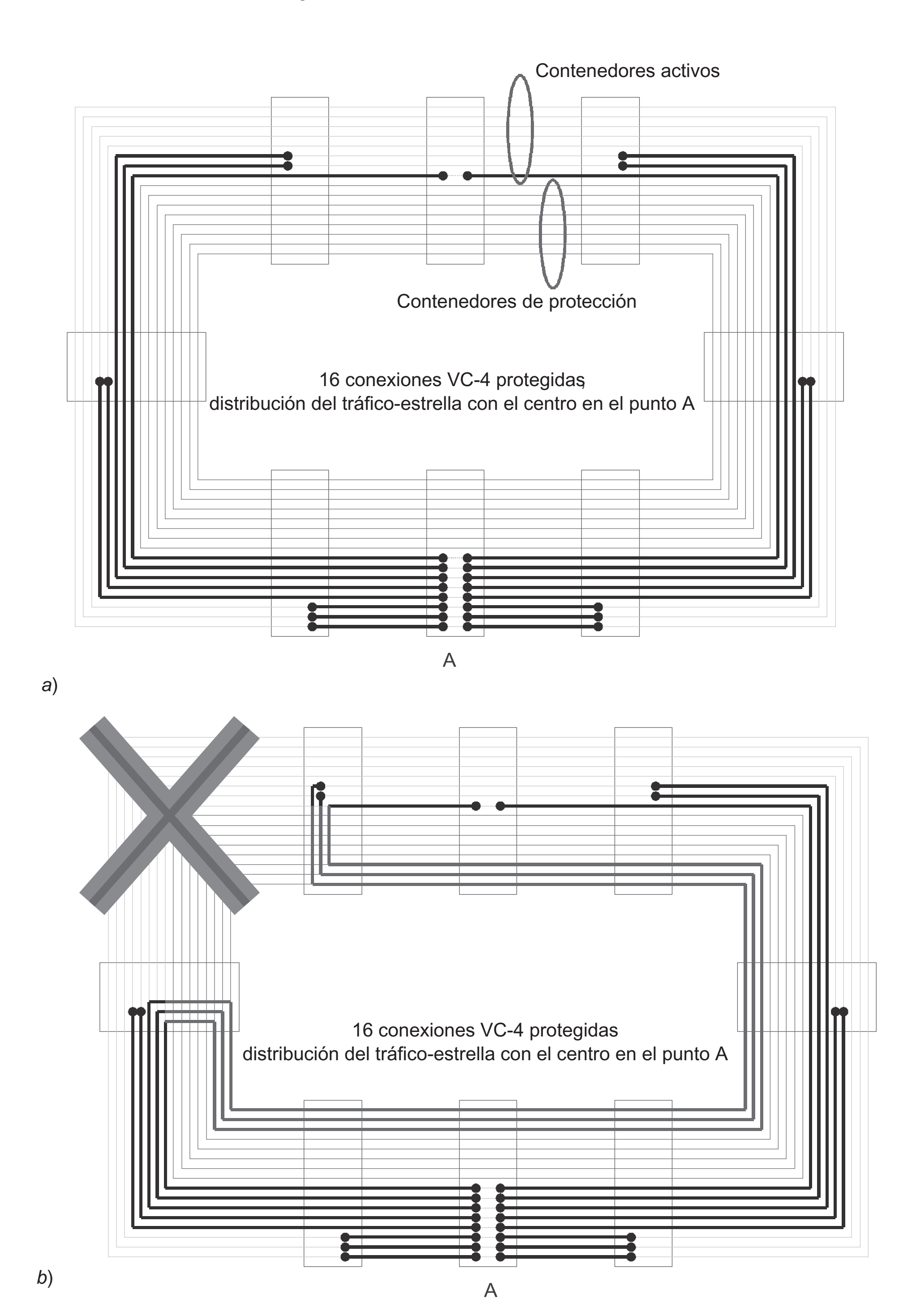


FIGURA 11.12 MS SPRing, protección con compartimiento de anillo.

multiplexor A es el centro en el que se concentra todo el tráfico, mientras que las mismas 16 conexiones de protección se establecen en el anillo como en el ejemplo del SNC-P que se observa en la figura 11.11. Para efectos de la protección de las conexiones se reservan 8 de 16 contenedores virtuales del flujo agregado STM-16.

En caso de falla o mal funcionamiento —como una falla en el enlace (figura 11.12*b*)—, el tráfico en los multiplexores cuya conexión esté dañada se invierte en la dirección opuesta. Esto se logra al usar contenedores virtuales de protección de los puertos agregados a los que se encuentran conectados los contenedores de las conexiones afectadas. Todas las conexiones que no se afectaron por la falla continúan trabajando de modo normal, sin tener que utilizar contenedores de protección. El protocolo del byte K se usa para notificar a los multiplexores acerca de la reconfiguración del anillo. El tiempo de conmutación de las conexiones de protección del método MS-SPRing es de alrededor de 50 milisegundos. Cuando se emplea la distribución de tráfico combinado, la economía del ancho de banda en el MS-SPRing puede ser aún más significativa.

11.4 REDES DWDM

PALABRAS CLAVE: multiplexaje por división de onda (WDM), multiplexaje por división de onda densa (DWDM), WDM de alta densidad, canal espectral separado, amplificador de fibra óptica, red totalmente óptica, multiplexor terminal, unidad de multiplexaje/demultiplexaje, amplificador de entrada, amplificador, preamplificador, conjunto de transpondedores, interfaz de color, red con conexiones intermedias, multiplexores ópticos de agregar/quitar, conexiones ópticas cruzadas, topología de anillo, topología de malla, filtro de película delgada, rejilla de difracción de fase, rejillas con arreglos de guías de onda (AWG), switches fotónicos, ruteadores de onda, ruteadores lambda y sistemas microelectromecánicos (MEMS).

La **tecnología del multiplexaje por división de onda densa** (**DWDM**) está diseñada para crear troncales ópticas de nueva generación, que operan a velocidades del orden de megabits o terabits. Dicho salto revolucionario en cuanto al desempeño está garantizado por este método de multiplexaje, el cual es básicamente distinto del que utilizan las redes SDH. En las redes DWDM, la información en la fibra óptica se transmite de manera simultánea mediante numerosas ondas luminosas: *lambdas* (la forma de designar la longitud de onda adoptada por la física: λ).

Las redes DWDM trabajan de acuerdo con el principio de conmutación de circuitos y cada onda luminosa constituye un canal espectral independiente. Cada onda transporta su propia información.

El equipo DWDM no está involucrado en forma directa en la resolución de problemas relacionados con la transmisión de datos en cada longitud de onda, esto es, en la selección del método para codificar la información y el protocolo de su transmisión. Sus principales funciones son las operaciones de *multiplexaje* y *demultiplexaje*, es decir, la combinación de diferentes ondas dentro del mismo flujo de señales y la separación de la función de cada canal espectral de la señal agregada. Los dispositivos DWDM más avanzados pueden también conmutar ondas.

NOTA *La tecnología DWDM no sólo es innovadora porque incrementa el límite de velocidad de la transmisión de datos a través de la fibra óptica decenas de veces, sino también porque inicia una nueva era en las técnicas de multiplexaje y conmutación, ya que lleva a cabo estas operaciones a través de señales luminosas sin transformarlas en*

señales eléctricas. Los demás tipos de tecnologías que utilizan señales luminosas para transmitir información a través de fibras ópticas, como SDH o Gigabit Ethernet, deben transformar las señales ópticas en eléctricas y solamente hasta entonces pueden llevar a cabo las operaciones de multiplexaje y conmutación.

La primera aplicación de la tecnología DWDM fue en troncales de larga distancia diseñadas para conectar dos redes SDH. Con esta topología punto a punto más simple, la capacidad de los dispositivos DWDM para llevar a cabo la conmutación de ondas es redundante. Sin embargo, a medida que la tecnología avanza y la topología de las redes DWDM se hace más compleja, esta función es cada vez más necesaria.

11.4.1 Principios de operación

En la actualidad, el equipo DWDM permite la transmisión, mediante el uso de una fibra óptica, de 32 o más ondas de varias longitudes en la ventana de transmisión de 1 550 nm, donde cada onda puede transportar información a una velocidad de hasta 10 Gbps (cuando se utilizan los protocolos de STM o 10 Gigabit Ethernet para transmitir información a cualquier longitud de onda). Las investigaciones actuales tienen como objetivo incrementar la velocidad de transmisión de información en cada longitud de onda dentro del rango de 40 a 80 Gbps.

El predecesor de DWDM fue la tecnología de **multiplexaje por división de longitud de onda** (**WDM**), la cual utiliza cuatro canales espectrales en la ventana de transmisión de 1 310 a 1 550 nm, con un espaciamiento entre las portadoras de 800 y 400 Ghz. (Debido a que no existe una clasificación WDM estándar se pueden encontrar dichos sistemas con otras características.)

El multiplexaje DWDM se le denomina como denso debido a que utiliza una distancia significativamente más pequeña entre longitudes de onda que las empleadas en WDM. En la actualidad, la recomendación G.692 de la ITU-T define dos rejillas de frecuencias (longitud de onda) (es decir, conjuntos de frecuencias separadas entre sí por cierto valor):

- Rejilla de frecuencias con un espaciamiento entre canales adyacentes de 100 GHz ($\Delta\lambda$ = 0.8 nm), de acuerdo con el cual se usan 41 ondas en el rango de 1 528.77 nm (196.1 THz) a 1 560.61 nm (192.1 THz).
- Rejillas de frecuencias con un espaciamiento de 50 GHz ($\Delta\lambda$ = 0.4 nm), que permiten transmitir longitudes de onda en el mismo rango.

Algunas compañías también fabrican equipo conocido con el nombre de **WDM de alta densidad**, capaz de trabajar con un paso de frecuencia de 25 GHz (por el momento, son en esencia dispositivos experimentales, por lo cual no se fabrican en forma masiva).

La implementación de las rejillas de frecuencias con pasos de 50 y 25 GHz determina requerimientos muy estrictos al equipo DWDM, en especial cuando cada onda transporta señales a una velocidad de modulación de 10 Gbps o mayor (STM-64, 10GE o STM-256). De nuevo, cabe hacer énfasis en que la tecnología DWDM (como la WDM) no está involucrada en forma directa en la codificación de la información que se transporta en cada longitud de onda. Este problema es resuelto por las tecnologías de las capas superiores, las cuales utilizan las longitudes de onda reservadas conforme se necesitan para transmitir información analógica o digital. Dichas tecnologías pueden ser SDH o 10 Gigabit Ethernet.

En teoría, las bandas de 50 GHz o aun la de 25 GHz entre longitudes de onda adyacentes permiten que los datos sean transmitidos a una velocidad de 10 Gbps. Sin embargo, en este

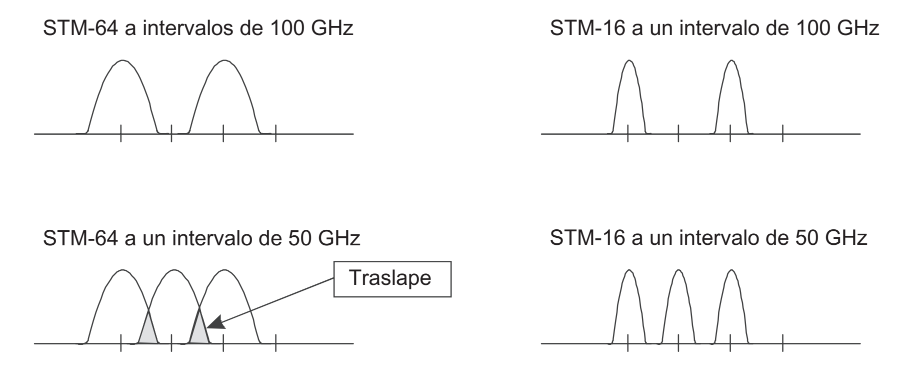


FIGURA 11.13 Superposición del espectro de longitudes de onda adyacentes para diferentes planos de frecuencia y velocidades de transmisión.

caso, es necesario garantizar una alta precisión de frecuencia y un mínimo valor de ancho espectral; además, se debe reducir el nivel de ruido con el fin de minimizar el efecto del traslapamiento de los espectros (figura 11.13).

11.4.2 Amplificadores de fibra óptica

El éxito de la tecnología DWDM en la práctica, cuyo equipo trabaja como troncal en la redes de la mayoría de los prestadores de servicios de comunicaciones más avanzados, ha determinado en muchos aspectos la aparición de los *amplificadores de fibra óptica*. Dichos dispositivos ópticos amplifican directamente las señales de luz en el rango de 1 550 nm, con lo que eliminan la necesidad de la conversión intermedia de dichas señales a señales eléctricas, como es el caso de los regeneradores que se utilizan en las redes SDH. Además, los sistemas de regeneración de señales eléctricas son costosos y dependen del protocolo debido a que necesitan percibir un método específico de codificación de las señales. Los amplificadores ópticos, los cuales transmiten información "de manera transparente", permiten aumentar la velocidad de transmisión en la troncal sin tener que actualizar las unidades amplificadoras.

La longitud de la sección entre dos unidades de amplificación óptica puede alcanzar un valor de 150 km o más, lo cual garantiza la eficiencia económica de las troncales DWDM, en las que la longitud de una sección de multiplexaje es de 600 a 3 000 km, siempre y cuando se utilicen de uno a siete amplificadores ópticos intermedios.

La recomendación G.692 del ITU-T define tres tipos de secciones amplificadoras (es decir, secciones entre dos multiplexores DWDM vecinos):

- **Larga (L):** la sección abarca ocho tramos de enlace de comunicaciones por fibra óptica y siete amplificadores ópticos. La distancia máxima entre amplificadores es de hasta 80 km, lo que hace una longitud máxima de la sección igual a 640 km.
- **Muy larga (V):** la sección incluye no más de cinco tramos de línea de comunicación por fibra óptica y cuatro amplificadores ópticos. La distancia máxima entre amplificadores es de hasta 120 km y la longitud máxima de la sección es de 600 km.
- **Ultralarga (U):** la sección no contiene amplificadores intermedios y tiene una longitud de 160 km.

Las limitaciones en cuanto al número de secciones pasivas y sus longitudes están relacionadas con la degradación de la señal óptica durante el proceso de amplificación óptica. A pesar de que el amplificador óptico EDFA restablece la potencia de la señal, no compensa por completo el efecto de la dispersión[1] cromática y otros efectos no lineales. Debido a lo anterior, en la construcción de troncales de larga distancia, es necesario instalar multiplexores DWDM entre las secciones amplificadoras. Éstos se encargan de regenerar la señal y la convierten a su forma eléctrica y, después, de nueva cuenta a su forma óptica. Con la finalidad de reducir los efectos no lineales, los sistemas DWDM también implican una limitación en la potencia de la señal.

Los amplificadores ópticos no sólo se utilizan para incrementar la distancia entre multiplexores, sino que también se usan dentro de los multiplexores. Aunque el multiplexaje y la conmutación cruzada se lleva a cabo exclusivamente con herramientas ópticas sin transformar las señales a su forma eléctrica, las señales pierden potencia en el proceso de las conversiones ópticas pasivas y éstas deben amplificarse antes de ser enviadas hacia la línea.

Investigaciones recientes en el campo de los amplificadores ópticos han dado como consecuencia la aparición de amplificadores que trabajan en el rango L (la cuarta ventana de transmisión), que va de los 1 570 a los 1 605 nm. El uso de este rango, así como la reducción del espaciamiento entre longitudes de onda de 50 y 25 Ghz permiten que el número de longitudes de onda transmitidas de manera simultánea se incremente a 80 o más. Esto significa que es posible garantizar la transmisión de tráfico a velocidades de 800 Gbps, 1.6 Tbps en una dirección a través de una sola fibra óptica.

El éxito de DWDM ha dado pie a la aparición de otra área tecnológica muy prometedora: las **redes totalmente ópticas**. En dichas redes, todas las operaciones relacionadas con el multiplexaje/demultiplexaje y conmutación cruzada/enrutamiento de la información del usuario se realizan sin transformar la señal óptica a una eléctrica. La eliminación de las transformaciones de la señal a su equivalente eléctrico garantiza la posibilidad de reducir de manera significativa los costos de la red. Por desgracia, el nivel actual de las tecnologías ópticas no es suficiente para construir redes totalmente ópticas en gran escala. Por lo tanto, el uso práctico de dichas redes está limitado por los segmentos ópticos por completo a través de los cuales la señal se regenera a nivel eléctrico.

11.4.3 Topologías típicas

Desde el punto de vista cronológico, la primera área de aplicación de DWDM (de manera similar a SDH) fue la construcción de troncales de alta velocidad y de longitud enorme con topología de **cadena punto a punto** (figura 11.14).

Para administrar dicha troncal, es suficiente instalar multiplexores DWDM terminales en sus puntos extremos. En los puntos de tránsito se deberán instalar amplificadores ópticos si la distancia entre los puntos terminales excede las limitaciones de distancia.

Un multiplexor terminal está formado por:

- Una unidad multiplexora/demultiplexora
- Un amplificador de entrada o impulsores (B)
- Un preamplificador (P)
- Un conjunto de transpondedores (T)

[1] La dispersión cromática se presenta debido a la diferencia de las velocidades de propagación de las ondas de luz que tienen longitudes diferentes. Por ello, la señal en el extremo receptor de la fibra se "dispersa".

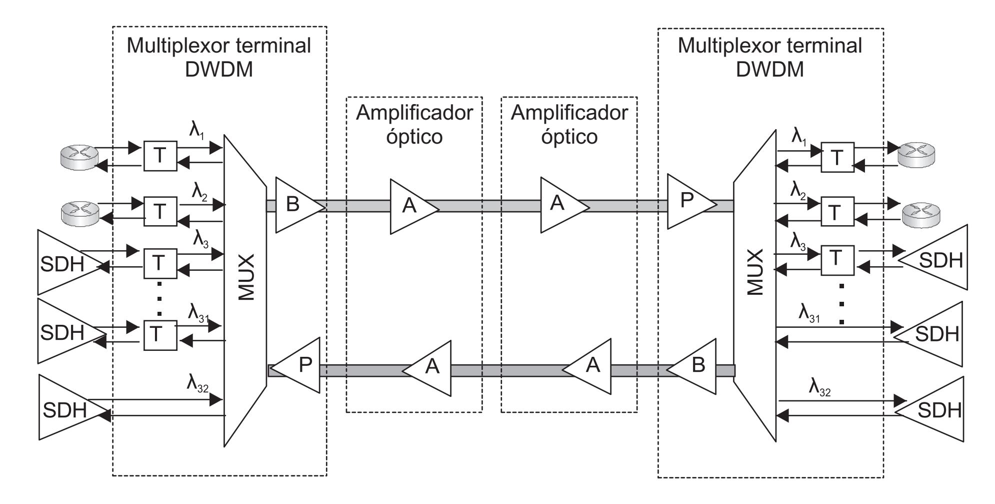


FIGURA 11.14 Troncal punto a punto de ultralarga distancia basada en multiplexores terminales DWDM.

Los transpondedores convierten las señales de entrada de las fuentes cuyas longitudes de onda no corresponden a la malla de frecuencias del multiplexor en ondas con la longitud requerida. Cuando el dispositivo conectado a la red DWDM puede generar la señal a una de las longitudes de onda soportadas por el multiplexor DWDM (de acuerdo con la rejilla de frecuencias de la recomendación G.692 de la ITU-T o la rejilla de frecuencias de un fabricante específico), los transpondedores no se utilizan. En este caso, se dice que el dispositivo conectado a la red DWDM tiene una interfaz de *colores*.

En el método proporcionado con anterioridad, el intercambio dúplex entre los usuarios de la red se lleva a cabo a costa de la transmisión unidireccional de todas las ondas que pasan a través de las dos fibras. Existe otra variante de la operación de las redes DWDM cuando sólo se utiliza una fibra para realizar la comunicación entre nodos. El modo dúplex en este caso se garantiza por la transmisión de señales bidireccionales al emplear fibra: la mitad de las ondas del plan de frecuencias transmiten información en una dirección, y la otra mitad de las ondas utilizadas para la transmisión de datos lo hace en la dirección opuesta.

Red con conexiones intermedias. La red en la que los nodos de tránsito llevan a cabo funciones de multiplexores de adicionar/quitar es un diseño natural de la topología anterior (figura 11.15).

Multiplexores ópticos de adicionar/quitar. Los OADM pueden separar (quitar) una onda de una longitud específica de la señal óptica agregada y adicionar ahí una señal de la misma longitud de onda, de tal modo que el espectro de la señal de tránsito no cambie y la conexión pueda establecerse con uno de los abonados conectados a un multiplexor de tránsito. El OADM puede agregar o quitar ya sea por métodos ópticos o al convertir la señal a una forma eléctrica. Por lo general, los multiplexores de agregar/quitar totalmente ópticos (pasivos) pueden eliminar un pequeño número de ondas. Esto se debe a que cada operación de remoción requiere que la señal óptica pase a través del filtro óptico, el cual incrementa la atenuación de la señal. Si el multiplexor utiliza regeneración eléctrica de la señal se podrá eliminar cualquier número de ondas dentro de los límites del grupo de longitudes de onda disponibles, ya que la señal óptica de tránsito fue totalmente demultiplexada con anterioridad.

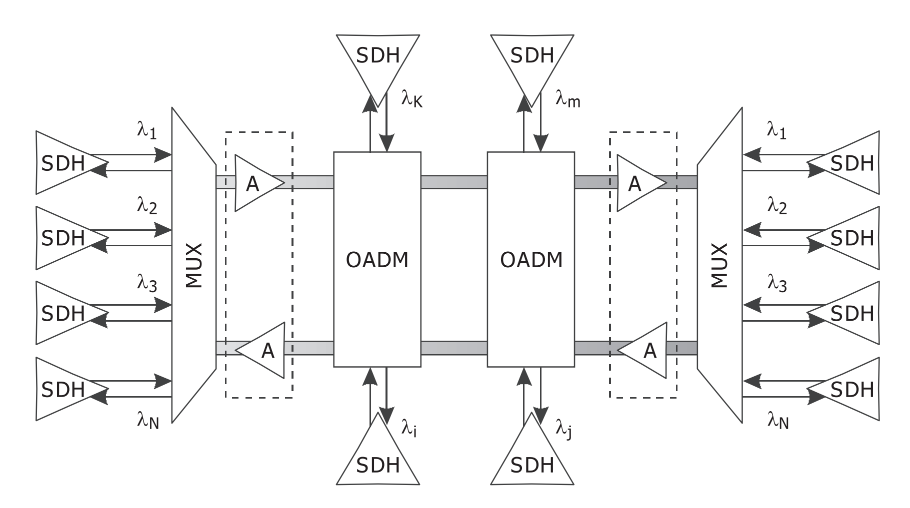


FIGURA 11.15 Red DWDM con multiplexores de adicionar/quitar en los nodos de tránsito.

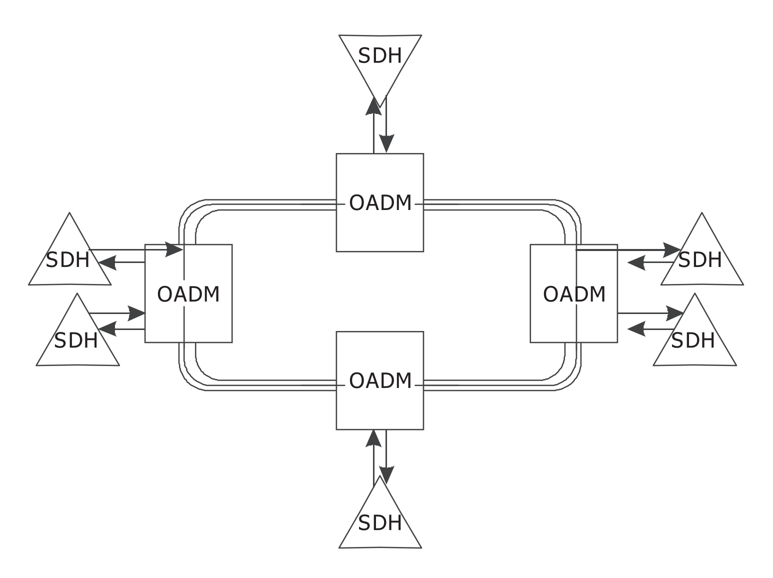


FIGURA 11.16 Anillo de multiplexores DWDM.

Anillo. La topología de anillo (figura 11.16) garantiza la supervivencia de la red DWDM debido a la presencia de trayectorias reservadas. Los métodos para desproteger el tráfico que se utilizan en DWDM son similares a los SDH (aunque en DWDM no están estandarizados todavía). Para resguardar una conexión específica se establecen dos trayectorias entre sus puntos terminales: el principal y el de protección. El multiplexor del punto terminal compara dos señales y selecciona la señal de mejor calidad (o la señal por omisión).

Topología en malla. Con la evolución de las redes DWDM, la topología en malla (figura 11.17) se utilizará en su diseño con más frecuencia debido a que ésta asegura una flexibilidad, desempeño y tolerancia a fallas mayor que otras topologías. Sin embargo, implementar la topología en malla requiere del empleo de **conexiones cruzadas ópticas** (OXC). Las OXC no solamente agregan y quitan ondas a y de la señal de tránsito agregada, como lo hacen los multiplexores adicionar/quitar, sino también soportan la conmutación arbitraria entre las señales ópticas transmitidas por las ondas de diferentes longitudes.

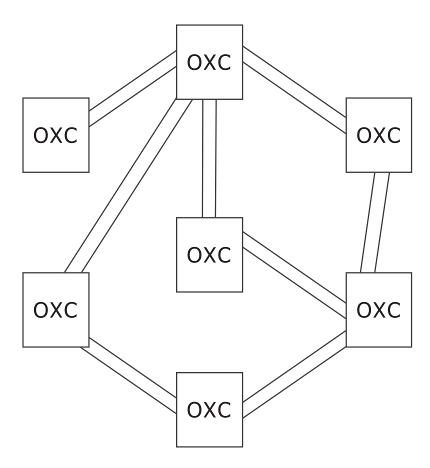


FIGURA 11.17 Topología en malla de la red DWDM.

11.4.4 Multiplexores ópticos de entrada/salida

Un multiplexor óptico multiplexa varias longitudes de onda en una señal agregada común y va quitando las ondas de diferentes longitudes de la señal agregada.

Para la remoción de ondas, el multiplexor puede utilizar varios mecanismos ópticos. En los multiplexores ópticos que soportan un número relativamente pequeño de longitudes de onda, por lo general de 16 a 32, se utilizan **filtros de película delgada**, los cuales forman las placas con un recubrimiento multicapa. En la práctica, los extremos de las fibras ópticas inclinados a un ángulo entre 30 y 45° y cubiertos con varias capas de recubrimiento se usan como filtros de película delgada. Para los sistemas con mayor número de longitudes de onda se requieren otros métodos de multiplexaje y filtrado.

En los multiplexores DWDM se utilizan las **rejillas de difracción de fase integrales** o **rejillas de arreglos de guías de onda** (**AWG**). Las funciones de las placas las llevan a cabo las guías de onda ópticas o las fibras. La señal entrante multiplexada es enviada al puerto de entrada (figura 11.18*a*). A continuación, esta señal pasa a través de la guía de ondas de la placa y se distribuye hacia un conjunto de guías de onda que representan la difracción de la estructura AWG. La señal en cada guía de ondas sigue siendo la multiplexada y cada canal (λ_1, λ_2,…λ_N) sigue presente en todas las guías de onda. Más adelante, las señales son reflejadas de la placa espejo y, por último, los rayos de luz se concentran de nuevo en la guía de onda de la placa. En este lugar, los rayos se enfocan y se lleva a cabo la interferencia. Como resultado, aparece la máxima interferencia, la cual se distribuye en el espacio. Dicha intensidad máxima corresponde a canales diferentes. La geometría de la guía de onda de placas —en particular, las posiciones de los polos de salida y los valores de las longitudes de las guías de onda AWG— se calcula para hacer que los máximos de interferencia coincidan con los polos de salida. El multiplexaje se lleva a cabo siguiendo el proceso inverso.

Otro método para construir el multiplexor se basa en el par de placas de guías de onda (figura 11.18*b*). El principio de operación de dicho dispositivo es similar al caso anterior, excepto por la placa adicional utilizada para efectos de enfoque e interferencia.

Las rejillas AWG integrales (también conocidas como fasores) se convirtieron en uno de los elementos clave de los multiplexores DWDM. Por lo general, se emplean para el demultiplexaje total de las señales luminosas, pues éstas pueden escalarse con éxito y son capaces de trabajar muy bien en sistemas con cientos de canales espectrales.

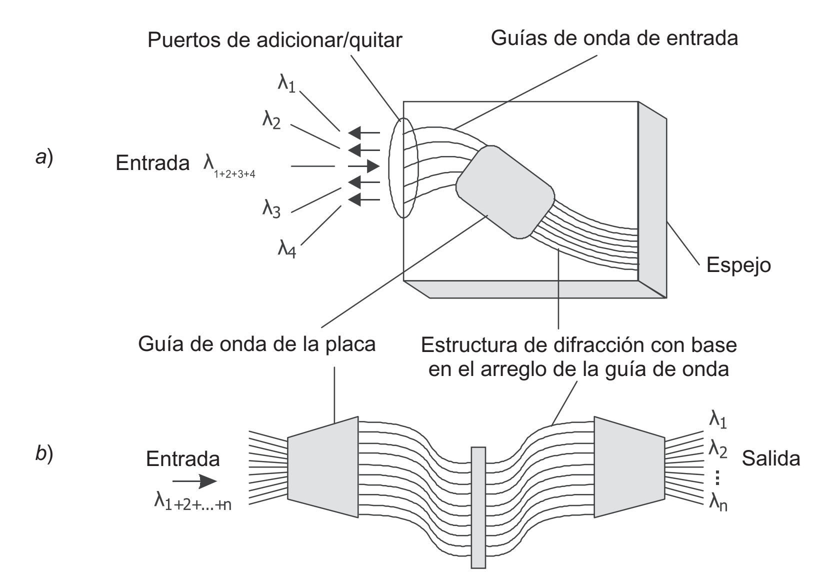


FIGURA 11.18 Demultiplexaje total de la señal con el uso de una rejilla de difracción de fase.

11.4.5 Conexiones cruzadas ópticas

En las redes con topología en malla es necesario asegurar las características de flexibilidad para cambiar la ruta de las conexiones de las ondas entre los abonados de la red. Dichas características son garantizadas por los OXC, los cuales permiten que cualquiera de las ondas de la señal de entrada a cualquier puerto se envíe a cualquiera de los puertos de salida (siempre y cuando ninguna otra señal de este puerto utilice dicha onda; de otra forma, será necesario traducir la longitud de onda).

Los OXC están dentro de las dos categorías siguientes:

- OXC con conversión intermedia de la señal a su forma eléctrica
- OXC totalmente ópticos

Las conexiones cruzadas optoelectrónicas fueron las primeras en aparecer y se nombraron OXC. Por lo tanto, los fabricantes de dispositivos totalmente ópticos de este tipo trataron de usar diferentes nombres para sus productos, como **switches fotónicos**, **ruteadores de ondas** o **ruteadores lambda**. Los OXC tienen una limitación principal: llevan a cabo su función de manera adecuada cuando trabajan a velocidades hasta de 2.5 Gbps; sin embargo, al comenzar a una velocidad de 10 Gbps, los tamaños de estos dispositivos y su consumo de energía exceden todos los límites. En los switches fotónicos, esta limitación no existe.

Con los switches fotónicos se utilizan varios mecanismos ópticos, incluidos las rejillas de difracción de fase y los **sistemas microelectromecánicos** (**MEMS**).

Los MEMS son el conjunto de pequeños espejos en movimiento, con no más de 1 mm de diámetro (figura 11.19). El interruptor MEMS se usa después del demultiplexor, donde la señal fuente se ha dividido en ondas componentes. Mediante el giro de un pequeño espejo a un ángulo específico, el rayo de la fuente de una longitud de onda específica se envía hacia la fibra de salida que le corresponde. Después, todos los rayos se multiplexan en la señal de salida agregada.

En comparación con los OXC, los switches fotónicos son cerca de 30 veces más pequeños y consumen alrededor de 100 veces menos energía. Sin embargo, este tipo de dispositivo tiene sus desventajas y una de las más importantes es su lenta respuesta y su sensibilidad a

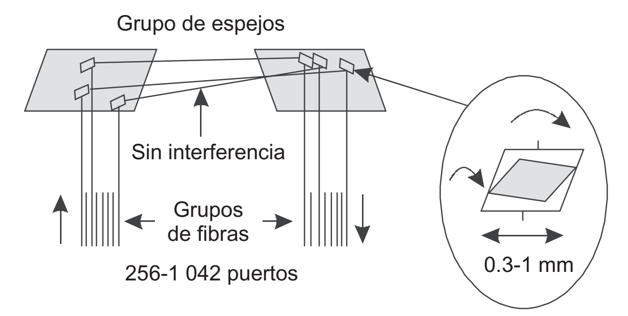


FIGURA 11.19 MEMS para la conmutación cruzada.

la vibración; no obstante, los MEM se usan ampliamente en nuevos modelos de switches fotónicos. En la actualidad, dichos dispositivos son capaces de garantizar la conmutación de canales espectrales de 256×256, y la aparición en el mercado de dispositivos que permitan conmutar $1\,024 \times 1\,024$ o mayores se espera en el corto plazo.

11.5 ESTUDIO DE UN CASO

El presente estudio de un caso describe la red de transmisión de una compañía energética de gran tamaño: ABC-Power. A pesar de que éste es un nombre inventado, como en todos los estudios de casos que se presentan en este libro, dichos estudios se basan en proyectos y sistemas del mundo real.

La compañía ABC-Power proporciona electricidad a una gran región que cubre cientos de kilómetros cuadrados. La compañía está formada por varias estaciones que generan energía, así como por la red de distribución que se utiliza para proporcionar energía a los clientes: grandes compañías y clientes independientes.

Las instalaciones de ABC-Power, las estaciones de energía y las estaciones distribuidoras están dispersas en 50 ciudades y establecimientos de la región. Para controlar el circuito de energía se utiliza un sistema de control jerárquico de tres niveles: el primero es el nodo central de administración, el segundo incluye los nodos regionales de control y el tercero consiste en estaciones de energía y de distribución. ABC-Power utiliza varias herramientas para la administración de los procesos de producción y distribución de energía, incluidos los siguientes:

- Sistemas de control automático y de telemetría para controlar diferentes instalaciones tecnológicas (estaciones de energía y distribución). Dichos sistemas están hechos de sensores que generan información en línea acerca del estado de los módulos de potencia y mecanismos activos que los controlan y llevan a cabo operaciones como la redistribución de potencia de una parte de la red de distribución a otra. Los datos de telemetría se transmiten entre las diferentes instalaciones en tiempo real y son proporcionados por la administración central y por los supervisores de las oficinas centrales y regionales.
- Comunicaciones especializadas para los despachadores, las cuales consisten en un sistema de comunicaciones de voz similar a la red telefónica, complementado por numerosas funciones que ayudan a los despachadores a resolver de manera coordinada los problemas que puedan surgir.
- Una red telefónica privada basada en PBX, la cual complementa las capacidades del sistema de comunicaciones del despachador y tiene una conexión a la red telefónica nacional.
- Un sistema de cómputo automatizado para administrar los recursos de la compañía.

Cada uno de los sistemas listados abarca subsistemas ubicados en los 50 puntos de presencia de ABC-Power. Resulta evidente que se requiere una red de telecomunicaciones de alta calidad para garantizar una operación estable de los sistemas de control y administración, los cuales conectan todos los puntos de presencia de ABC-Power mediante enlaces confiables de alta velocidad.

Por mucho tiempo, ABC-Power arrendaba enlaces de comunicaciones con velocidades de 64 Kbps a 2 Mbps del prestador regional de servicios de comunicaciones. Estos enlaces se utilizaban para conectar el PBX y los ruteadores /switches de las LAN. Los sistemas de control automático y telemétrico usaban parcialmente los enlaces de cobre que eran propiedad de ABC-Power. Dichos enlaces estaban instalados a lo largo de las líneas de transmisión de energía hacia las instalaciones ubicadas más allá de la zona a la que daba servicio el prestador regional de comunicaciones.

El desarrollo posterior del negocio de ABC-Power requirió emplear los métodos más avanzados de administración, incluidos la instalación de PBX digitales nuevos capaces de combinar las funciones de las comunicaciones del despachador y la telefonía convencional, el uso de un poderoso sistema de administración integrada SAP R/3 en lugar de sistemas de administración departamental aislados, y la mejora de la telemetría y de los sistemas de control automático.

Semejante modernización de herramientas administrativas requirió depurar los enlaces de comunicaciones, incluidos una confiabilidad mejorada y un incremento del ancho de banda.

Un análisis de las posibles variaciones en las mejoras de la infraestructura de los enlaces de comunicaciones demostró que el arrendamiento de enlaces de alta velocidad que garantizaran velocidades de 34 Mbps a 155 Mbps era ineficaz desde el punto de vista económico. Como resultado, ABC-Power decidió crear su propia red de transmisión aprovechando las ventajas de la red existente en cuanto a las líneas de transmisión de energía eléctrica. Este método fue seleccionado por muchas compañías de ferrocarril, energía eléctrica, petroleras y de gas. La instalación de fibra óptica a lo largo de la tubería existente de gas o del ferrocarril no requería una inversión significativa y por lo general se caracterizaba por un rápido retorno de la inversión.

La red de transmisión de ABC-Power fue construida en dos años. El cable de fibra óptica conectaba los multiplexores SDH en los 50 puntos de presencia de la compañía (figura 11.20).

Dicha red de transmisión tenía una topología en malla, la cual permite a la compañía aplicar los métodos de protección de enlaces de tecnología SDH y garantizar una alta confiabilidad. Se utilizaron tres tipos de multiplexores en la red: M4, M1 y MA. Los M4 son multiplexores adicionar/quitar de nivel STM-4, esto es, sus puertos agregados operan a una velocidad STM-4 (622 Mbps). Estos multiplexores forman el anillo troncal que conecta grandes nodos de control regionales, así como el nodo de control central. El multiplexor M4 tolera el reemplazo de los puertos agregados STM-4 con los puertos agregados STM-16 (2.5 Gbps), los cuales trabajan en una de las ondas del plan de frecuencias del DWDM. Esto garantiza la posibilidad de incrementar aún más la velocidad de la troncal de la red sin necesidad de reemplazar el equipo, incluida la posibilidad de conectar la red SDH a la troncal DWDM.

La red de acceso de transmisión está basada en el uso de multiplexores M1 y MA (puertos agregados a 155 Mbps STM-1). Esa red abarca todas las estaciones de energía y pequeños nodos de control regional y combina la topología en malla con la topología en árbol, con lo que asegura la redundancia sólo en las rutas más críticas. Los multiplexores MA se distinguen por sus numerosos puertos PDH utilizados para conectar el equipo de las redes superpuestas, como la de teléfono, de cómputo, telemétrica y de control (figura 11.21).

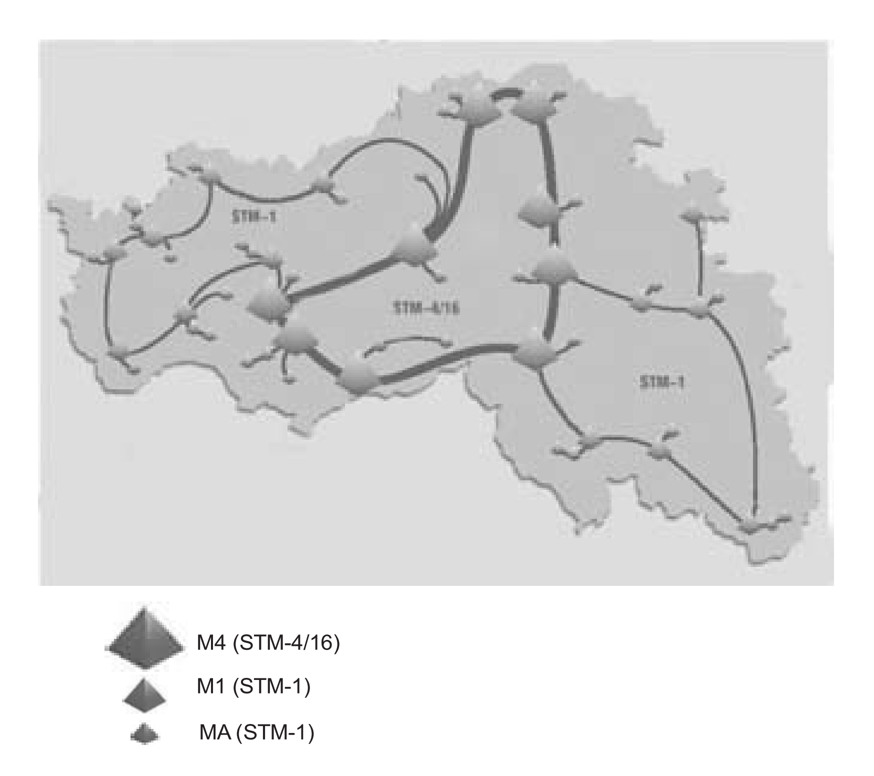


FIGURA 11.20 Transmisión en la red SDH de ABC-Power.

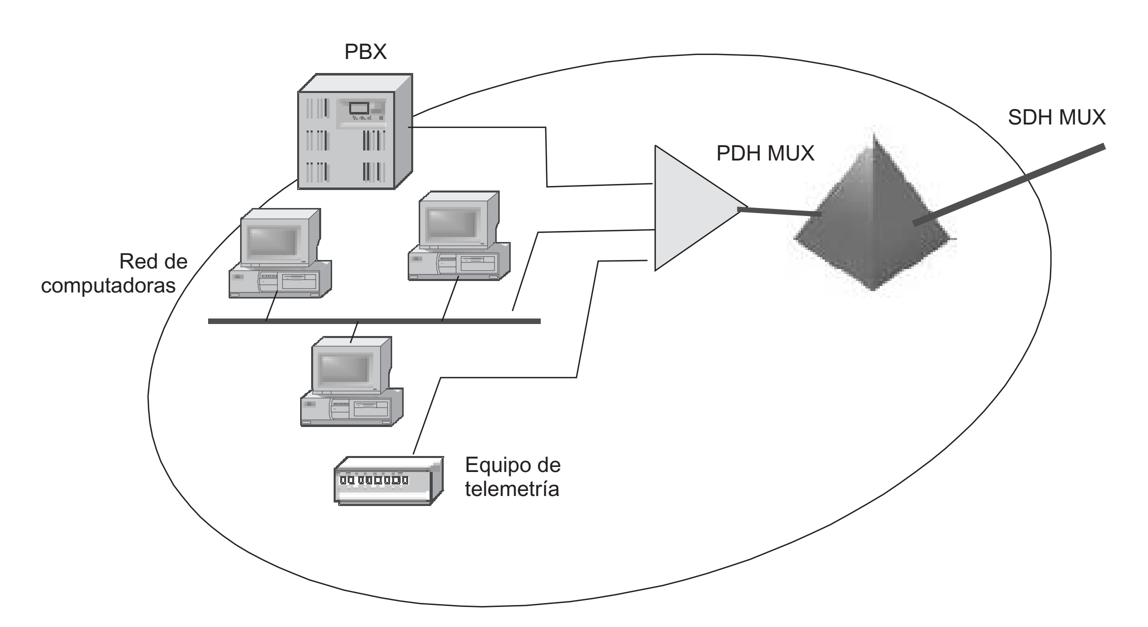


FIGURA 11.21 Conexión del equipo a la red SDH.

La creación de la red SDH privada permitió que ABC-Power estuviera a salvo cuando se evaluaron las necesidades de la compañía de instalar enlaces de comunicaciones de alta velocidad. La compañía planea utilizar los enlaces sobrantes en actividades comerciales como si fuera un proveedor de servicios de Internet.

RESUMEN

- Las redes de transmisión están diseñadas para crear infraestructura conmutada y utilizan lo que sea posible para crear de manera rápida y flexible canales persistentes para formar una topología arbitraria.
- Las redes de transmisión emplean variantes de las técnica de conmutación de circuitos, mediante el uso de multiplexaje por división de frecuencia (FDM), multiplexaje por división de tiempo o multiplexaje por división de onda/onda densa (WDM/DWDM).
- En las redes FDM, a cada loop local se le reserva la banda de frecuencias con un ancho de 4 kHz. Existe una jerarquía de canales FDM, donde 12 loops locales conforman los canales de primer nivel (el grupo base) con una frecuencia de 48 kHz. Cinco canales del primer nivel se agrupan en un canal de segundo nivel (el supergrupo) con una banda de frecuencia de 240 kHz. Diez canales de segundo nivel conforman el canal de la tercera capa jerárquica (el grupo principal) con una banda de frecuencia de 2.4 MHz.
- Las redes digitales de transmisión (PDH) permiten crear canales con una eficiencia que va desde 64 Kbps hasta 140 Mbps, con lo que ofrecen a sus suscriptores cuatro niveles de la jerarquía de velocidades.
- La desventaja de las redes PDH es la imposibilidad de separar de manera directa los datos del canal de baja velocidad de los de alta velocidad, ya que dichos canales operan en niveles no adyacentes de la jerarquía de velocidades.
- El modo asíncrono de suma de flujos de suscriptor en la trama SDH está garantizado por el concepto de contenedores virtuales y el sistema de apuntadores flotantes que indican el punto de comienzo de los datos del usuario en el contenedor virtual.
- Los multiplexores SDH pueden operar en redes con topologías diferentes, incluidas las de cadena, anillo y malla. Existen varios tipos especiales de multiplexores que ocupan un lugar específico en la red: multiplexores terminales, multiplexores adicionar/quitar y conexiones cruzadas (OXC).
- En las redes SDH, muchos mecanismos soportados relacionados con la tolerancia a fallas protegen el tráfico de datos a nivel de bloques, puertos y conexiones específicos: EPS, protección de tarjetas, MSP, SNC-P o MS-SPRing. El método más eficaz de protección se selecciona en función de la topología lógica de las conexiones de la red.
- La técnica de multiplexaje WDM/DWDM implementa los principios del multiplexaje en frecuencia para las señales de otra naturaleza física y en otro nivel de la jerarquía de velocidades. Cada canal WDM/DWDM es un rango específico de ondas de luz, que le permiten transportar datos en forma analógica o digital. Al mismo tiempo, el ancho de banda del canal es de 25-50-100 Ghz, lo cual garantiza velocidades de varios gigabits por segundo (cuando se transmiten datos en forma discreta).
- En los primeros sistemas WDM se utilizaba un pequeño número de canales espectrales, de 2 a 16. En la actualidad se usan de 32 a 160 canales en una sola fibra óptica, lo cual garantiza velocidades de datos de hasta varios terabits por segundo a través de una sola fibra.
- Los amplificadores de fibra actuales permiten que la sección óptica del enlace de conexión se extienda a 700-1 000 km sin tener que cambiar la señal a su forma eléctrica.
- Para separar varios canales de la señal luminosa agregada, suelen combinarse dispositivos relativamente baratos con amplificadores ópticos para administrar los multiplexores de agregar/quitar en las redes de larga distancia.

- Para la interacción con las redes ópticas convencionales (SDH, Gigabit Ethernet y 10 Gigabit Ethernet), las redes DWDM utilizan transpondedores y traductores de longitud de onda, los cuales transforman la longitud de onda de la señal de entrada en una de las longitudes de onda del plan estándar de frecuencia de DWDM.
- En las redes totalmente ópticas, todas las operaciones de multiplexaje y conmutación se llevan a cabo sobre las señales luminosas sin cambiar la señal a su formato eléctrico. Esto simplifica la red y reduce su costo.

PREGUNTAS DE REPASO

1. ¿Qué desventajas de las redes de transmisión FDM han dado como consecuencia la creación de las redes digitales de transmisión?
2. El nombre T-1 significa:
   a) Un equipo multiplexor diseñado por AT&T
   b) Un nivel de velocidad de 1.544 Mbps
   c) Un estándar internacional de un enlace de comunicaciones
   d) Un método de multiplexaje de flujos digitales de 64 Kbps
3. ¿Qué funciones se delegan al bit menos significativo de cada byte en el canal T-1 cuando se transmite voz?
4. ¿Es posible separar el canal DS-0 directamente del canal DS-3 en una red PDH?
5. ¿Qué métodos se utilizan en la práctica para resolver el problema anterior?
6. ¿Qué mecanismos están implementados en el canal E-1 para reemplazar el robo de bits del canal T-1?
7. ¿Por qué las redes de transmisión garantizan una alta calidad de servicio para todos los tipos de tráfico?
8. ¿Qué propiedad de la tecnología PDH se refleja con el término *presíncrono*?
9. ¿Cómo compensa la tecnología SDH la falta de sincronía en las ráfagas tributarias?

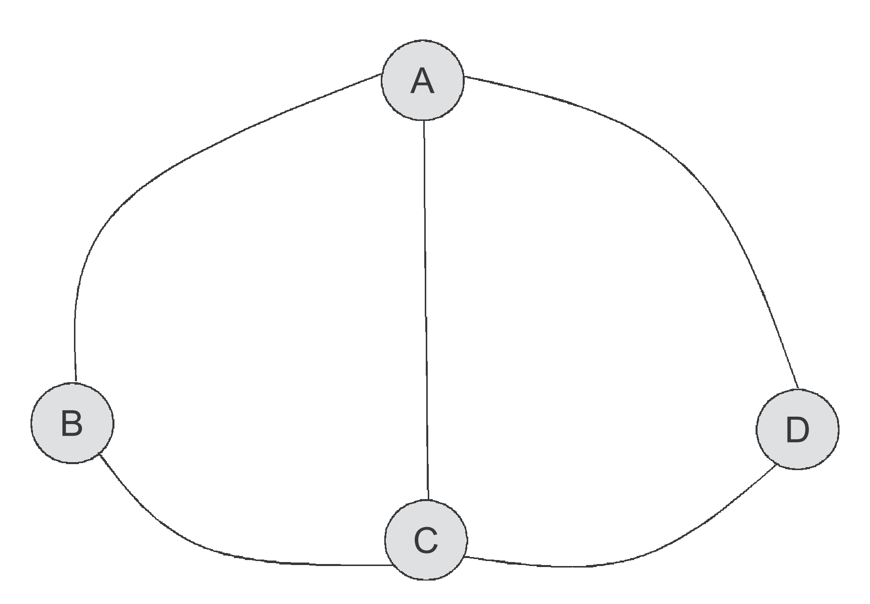


FIGURA 11.22 Distribución del tráfico.

10. ¿Cuál es el número máximo de canales E-1 que pueden ser multiplexados por la trama STM-1?
11. ¿Cuántos canales T-1 pueden ser multiplexados por la trama STM-1, siempre y cuando ésta tenga 15 canales E-1?
12. ¿Qué capas de la pila de protocolos SDH son responsables de reconfigurar la red en caso de una falla en el equipo?
13. ¿Cuál es la máxima velocidad del canal de comunicación de datos entre los regeneradores SDH?
14. ¿Por qué la trama STM-1 utiliza tres apuntadores?
15. ¿Cuál es el propósito de utilizar un byte entrelazado en las tecnologías PDH y SDH?
16. ¿Cuál es la diferencia entre los métodos de protección 1+1 y 1:1?
17. ¿En qué condiciones el MS-SPRing es más eficiente que el SNC-P?
18. ¿Cuáles son las características comunes entre las redes de transmisión FDM y DWDM?
19. ¿Qué tipos de redes son las DWDM: analógicas o digitales?
20. ¿Cuál es el objetivo de utilizar regeneradores que transformen una señal óptica en una eléctrica en las redes DWDM?
21. ¿Cuáles son las razones que provocan el deterioro de la señal óptica cuando pasa a través de muchas secciones DWDM pasivas?
22. ¿Qué principios de la conmutación de las señales de luz se utilizan en las OXC?

PROBLEMAS

1. ¿Cuál será la frecuencia del alineamiento negativo del apuntador de VC-4 en la trama STM-1 si la diferencia relativa entre las frecuencias de reloj de transmisión y de recepción de los multiplexores SDH es de 10^{-5}?
2. La red SDH abarca cuatro multiplexores STM-4: A, B C y D. La figura 11.22 muestra la distribución de tráfico entre ellos. Todos los flujos están a la velocidad STM-1 y los multiplexores se hallan conectados por el mismo anillo STM-4. ¿Qué método de protección deberá seleccionarse para proteger todas las conexiones?

PARTE III

REDES DE ÁREA LOCAL

Las LAN constituyen una parte integral de cualquier red de computadoras actual. Si observa la estructura de cualquier WAN, como Internet o simplemente una red corporativa muy grande, podrá notar que casi todos los recursos de información de la red están concentrados dentro de las LAN; la WAN es sólo el transporte que conecta a un gran número de LAN.

Uno de los objetivos más importantes de una LAN es conectar computadoras dentro de un edificio o grupos de edificios ubicados a cortas distancias entre sí con el fin de brindar a sus usuarios acceso a los servicios de información de los servidores locales. Las LAN también proporcionan un método idóneo de agrupar computadoras para conectarlas a una WAN, pues para una WAN es mucho más fácil enviar datos entre las redes que entre las computadoras individuales. Las LAN inalámbricas que proporcionan servicio a los aeropuertos o estaciones de ferrocarril son un buen ejemplo: como regla, dichas redes no están diseñadas para garantizar el intercambio de información entre usuarios temporales; por el contrario, su principal objetivo es ofrecer a los usuarios el acceso a Internet. Debe hacerse énfasis que en estos casos, el acceso a Internet está planeado para toda la LAN, en vez de estarlo para los usuarios individuales. Las LAN también se utilizan en otras redes de telecomunicaciones, como las telefónicas y las de transmisión. Por ejemplo, los sistemas que administran los switches telefónicos o las redes de transmisión en general están construidos con base en una LAN, la cual conecta las computadoras de operadores de red, garantizándoles de esta forma el acceso a los dispositivos de control incluidos en el equipo de las redes de telecomunicaciones.

Las tecnologías LAN han evolucionado a pasos agigantados. Prácticamente todas las tecnologías en la década de 1980 utilizaron el *medio de transmisión compartido* como una forma conveniente y económica para conectar computadoras en la capa física. Los principios básicos de los medios de transmisión compartidos se estudiaron en el *capítulo 2.* En esta parte del libro se reconsiderará el problema para profundizar más en los aspectos de estandarización y algoritmos específicos utilizados.

A mediados de la década de 1990, las LAN comenzaron a usar *versiones conmutadas* de las tecnologías. Dejar a un lado el empleo del medio de transmisión compartido ayudó a mejorar el desempeño y escalabilidad de las LAN. Las LAN conmutadas utilizan los mismos protocolos que las LAN de medio de transmisión compartido, pero en modo *full-dúplex*. Otra ventaja de las LAN conmutadas consiste en los diferentes métodos que ésta utiliza para garantizar la calidad del servicio (QoS); esto es en particular importante cuando una LAN transmite tráfico en tiempo real, por ejemplo: tráfico telefónico IP.

A pesar de la popularidad de las LAN conmutadas, el medio de transmisión compartido aún se utiliza con frecuencia en las tecnologías convencionales y modernas. Éstas son eficientes en pequeños segmentos de las LAN cableadas, así como en las LAN inalámbricas, donde el medio de transmisión es compartido por naturaleza.

Las LAN no sólo experimentan cambios en el uso de los medios de transmisión: la velocidad máxima de transferencia de información de los protocolos de las LAN también está en aumento. Con la adopción del estándar 10G Ethernet en 2002, los estándares de las LAN comenzaron a soportar una jerarquía de velocidades que está a la par con las de las redes de transmisión: de 10 Mbps a 10 Gbps. Esto permite construir MAN y LAN con base en dichas tecnologías.

La evolución de las LAN tiende también hacia la miniaturización. Ha aparecido un nuevo tipo de red: la *de área personal*, la cual conecta los dispositivos electrónicos de un solo usuario dentro de un rango de varios cientos de metros.

Las LAN modernas existen en condiciones dominadas por una tecnología de red o, para ser más precisos, por una familia entera de tecnologías de red: Ethernet. Naturalmente, a

esta familia de tecnologías se le dedica mucho más atención en este libro que a cualquiera de las demás. La parte III incluye los capítulos siguientes:

- El capítulo 12 (Ethernet) abarca la clásica tecnología Ethernet a 10 Mbps, basada en un medio de transmisión compartido.
- El capítulo 13 (Ethernet de alta velocidad) estudia las tecnologías Ethernet de alta velocidad basadas en el uso de un medio de transmisión compartido: Fast Ethernet y Gigabit Ethernet.
- El capítulo 14 (LAN de medios compartidos) describe otras tecnologías LAN basadas en un medio de transmisión compartido (Token Ring y FDDI) y dos tecnologías inalámbricas: IEEE 802.11 y Bluetooth.

En los dos últimos capítulos se analizan las LAN conmutadas.

- En el capítulo 15 (Fundamentos de LAN conmutada) se estudian los fundamentos de la operación de las LAN conmutadas: su algoritmo de trabajo, las versiones full-dúplex de los protocolos de las LAN y las características específicas de implementación de los switches en este tipo de redes.
- En el capítulo 16 (Características avanzadas de LAN conmutadas) se examinan las propiedades avanzadas de las LAN de este tipo, incluidos los enlaces redundantes con base en el algoritmo del árbol extendido, la adición de enlaces y la técnica de las VLAN.

12

ETHERNET

DESCRIPCIÓN DEL CAPÍTULO

12.1 INTRODUCCIÓN

Ethernet es en la actualidad el estándar más conocido de LAN: se estima que el número total de redes que utilizan el protocolo Ethernet es de varios millones.

El término Ethernet por lo regular se refiere a una variante de la tecnología; las variantes incluyen Fast Ethernet, Gigabit Ethernet y 10G Ethernet.

En un sentido restringido, *Ethernet* es un estándar de red para transmitir datos a una velocidad de 10 Mbps que apareció a finales de la década de 1970 como un estándar propietario de tres compañías: Digital Equipment Corp. (DEC), Intel y Xerox. A principios del decenio de 1980, Ethernet fue estandarizado por el grupo de trabajo IEEE 802.3 y desde entonces se ha convertido en un estándar internacional. Ethernet fue la primera tecnología que sugirió usar un medio de transmisión compartido para tener acceso a la red.

Como son una red de conmutación de paquetes, las LAN emplean el principio del multiplexaje por división de tiempo, lo cual significa que comparten el medio de transmisión en tiempo. El algoritmo para compartir el tiempo, el control de acceso al medio de transmisión (MAC), es una de las características más importantes de cualquier tecnología LAN, debido a que tiene una influencia mucho mayor en el tipo de tecnología que el método de codificación de las señales o el formato de trama. Ethernet utiliza un método de acceso aleatorio como mecanismo para compartir el medio de transmisión: aunque está muy lejano de ser perfecto, ya que el ancho de banda efectivo de la red disminuye de manera notable a medida que la carga de la red aumenta, la razón principal del éxito de Ethernet fue su simplicidad.

La amplia aceptación de la red Ethernet a 10 Mbps sirvió como incentivo eficaz para su desarrollo: el estándar Fast Ethernet fue adoptado en 1995, el Gigabit Ethernet apareció en 1998 y el 10G Ethernet en 2000. Cada uno de los estándares más actuales fue 10 veces más rápido que su predecesor, con lo cual se generó una jerarquía de velocidades impresionante:

10 Mbps – 100 Mbps – 1 000 Mbps – 10 000 Mbps

En este capítulo se estudia en detalle la tecnología Ethernet a 10 Mbps clásica, cuyos principios se emplean a velocidades de transmisión muy elevadas.

12.2 CARACTERÍSTICAS GENERALES DE LOS PROTOCOLOS LAN

PALABRAS CLAVE: medio de transmisión de datos compartido, topologías estándar de conexiones físicas, pila de protocolos LAN, control del enlace lógico (LLC, por sus siglas para Logical Link Control), control de acceso al medio (MAC, Médium Access Control), acceso aleatorio, acceso determinístico, colisión, algoritmo de poleo, árbitro, demultiplexaje, multiplexaje, punto de acceso del servicio de destino (DSAP, o destination service access point), punto de acceso al servicio de la fuente (SSAP, por source service access point), LLC1, LLC2, LLC3, estándares IEEE 802.x, y modo de transmisión de datagramas half-dúplex.

Ethernet pertenece a toda la familia de tecnologías LAN, la cual también incluye Token Ring, FDDI, IEEE 802.11 y 100VG-AnyLAN.[1] A pesar de algunas de sus características específicas, todas estas tecnologías tienen el mismo propósito: la construcción de LAN. Por lo tanto, tiene sentido comenzar con el estudio de Ethernet y observar los principios generales utilizados en el desarrollo de las tecnologías LAN.

[1] La tecnología 100VG-AnyLAN está prácticamente en desuso en la actualidad. No obstante, el concepto original de compartición del medio de transmisión implementado en dicha tecnología es de interés teórico.

12.2.1 Topologías y medios de transmisión compartidos estándares

El objetivo primordial que los diseñadores de las primeras LAN tuvieron que alcanzar a finales de la década de 1970 fue encontrar una solución sencilla y barata para conectar cientos de computadoras ubicadas dentro del mismo edificio en una red de computadoras. La solución tenía que ser barata, pues la red iba a servir para conectar minicomputadoras de bajo costo (en comparación con las computadoras grandes o *mainframes*), las cuales ya habían aparecido en el mercado y su uso se hizo muy popular rápidamente (el costo de cada una se hallaba en el rango de $10 000 a $20 000). El número de dichas computadoras instaladas en una sola organización era reducido; por lo tanto, como máximo varios cientos de computadoras parecían suficientes para casi cualquier LAN. El problema que representaba conectar LAN para formar WAN no era una prioridad en ese tiempo, por lo cual la mayoría de las tecnologías LAN lo ignoraron.

Para efectos de simplicidad y, en consecuencia, de reducción de costos en hardware y software, los diseñadores de las primeras LAN decidieron utilizar un **medio de transmisión de datos compartido**.

Este método de administración de las comunicaciones entre computadoras fue probado por primera vez con la red de radio ALOHA en la Universidad de Hawai con la supervisión de Norman Abramson a principios de la década de 1970. Un canal de radio de una banda de frecuencia específica opera de manera natural como medio de transmisión compartido para todos los transmisores que utilizan frecuencias de dicha banda para la codificación de datos. La red ALOHA empleaba el método de acceso aleatorio, de acuerdo con el cual cualquier nodo podía iniciar la transmisión de un paquete en cualquier momento. Si el nodo no recibía una confirmación antes de que expirara cierto tiempo, el paquete se retransmitía. El medio de transmisión compartido era un canal de radio con una frecuencia portadora de 400 MHz y un ancho de banda de 40 KHz, lo que garantizaba una velocidad de transmisión de datos de 9 600 bps.

Tiempo después, Robert Metcalfe puso en práctica la idea de un medio de transmisión compartido para las LAN cableadas: un segmento continuo de cable coaxial se convirtió en el medio de transmisión análogo al medio por radio. Todas las computadoras estaban conectadas a este segmento de acuerdo con el diseño de una compuerta `OR` cableada (figura 12.1). Por esta razón, cuando un transmisor enviaba señales, todos los receptores recibían la misma señal, de forma parecida a cuando se utilizaban ondas de radio.

En las redes Token Ring y FDDI, el hecho de que todas las computadoras utilicen un medio de transmisión compartido no es tan significativo como lo es para Ethernet. Las redes se basan en una topología física en anillo, en la cual cada nodo está conectado mediante un cable a los dos nodos vecinos (figura 12.2). Sin embargo, estas secciones de cable también están compartidas, pues en cualquier momento sólo una computadora puede utilizar el anillo para transmitir paquetes.

Topologías estándar simples de conexiones físicas (estrella en Ethernet con coaxial y anillo en Token Ring y FDDI) garantizan la facilidad de uso del cable como medio de transmisión compartido.

El uso de un medio de transmisión compartido *simplifica* la lógica de la operación de los nodos de la red. Como sólo una operación de transmisión de datos puede estar en proceso

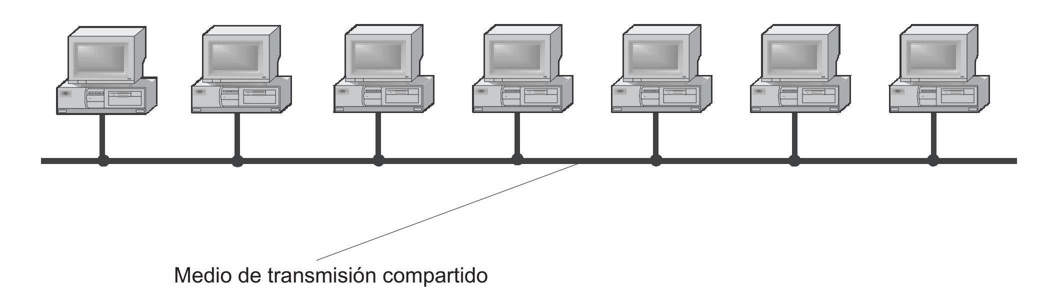


FIGURA 12.1 Medio de transmisión compartido con base en cable coaxial.

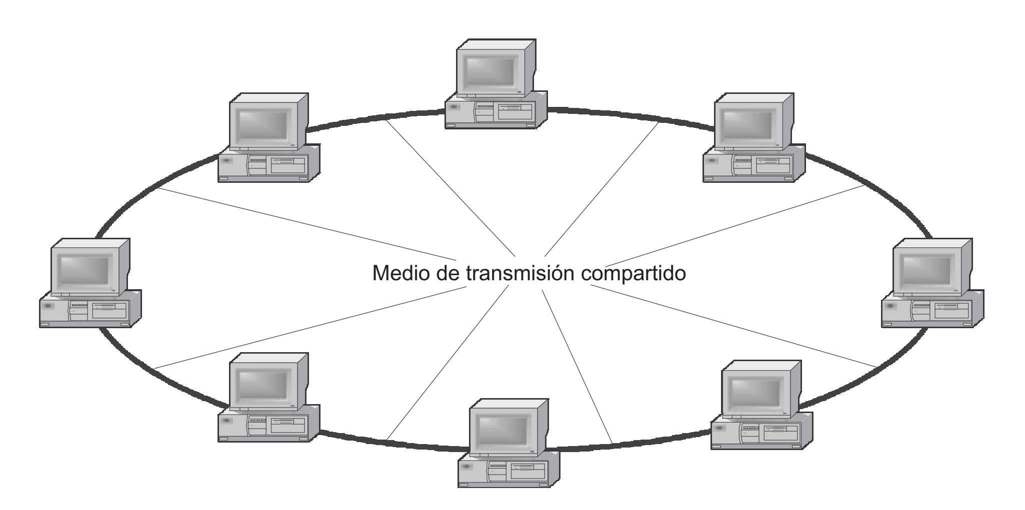


FIGURA 12.2 Medio de transmisión compartido en topologías anillo.

a la vez, no es necesario almacenar tramas en los nodos de tránsito. Además, no existen nodos de tránsito (esta variante poco usual de red de conmutación de paquetes se estudió en el capítulo 2). En consecuencia, ya no existe la necesidad de contar con procedimientos complejos para administrar el flujo ni para controlar la congestión.

La desventaja principal del medio de transmisión compartido es su *pobre escalabilidad*. Dicha desventaja es importante debido a que el ancho de banda de este medio de transmisión está dividido entre todos los nodos de la red sin considerar el método de acceso al medio de transmisión que se emplee. En este caso, se puede usar el resultado que se obtuvo al aplicar la teoría de colas descrita en el capítulo 7: en cuanto el coeficiente de utilización del medio compartido exceda cierto nivel, las colas para acceder al medio de transmisión comenzarán a crecer de manera no lineal. Como resultado, la red resulta prácticamente inútil. El valor del umbral del coeficiente de utilización depende del método de acceso empleado. Por ejemplo, en las redes ALOHA, este valor es muy bajo (alrededor del 18%). En Ethernet, este valor es mayor (alrededor de 30%) y en las redes Token Ring y FDDI alcanza un valor entre 60 y 70%.

12.2.2 Pilas de protocolos de las LAN

Como regla general, las topologías LAN implementan sólo las funciones de las dos capas inferiores del modelo OSI, esto es, de las *capas física* y de *enlace de datos* (figura 12.3). Ello se

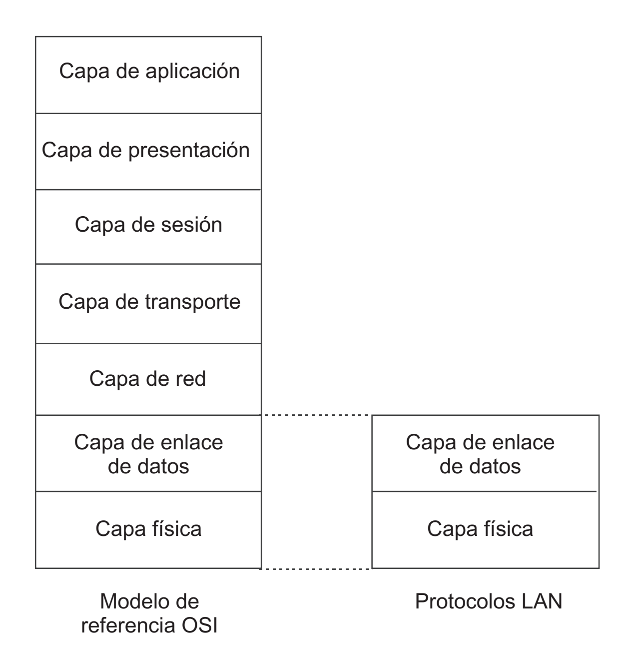


FIGURA 12.3 Correspondencia entre los protocolos LAN y las capas del modelo OSI.

debe a que la funcionalidad de estas dos capas es suficiente para la entrega de tramas dentro de la estructura de las topologías LAN estándares: estrella (bus común), anillo y árbol.

A pesar de lo anterior, eso no significa que las computadoras conectadas a través de una LAN no soporten los protocolos de las capas que están arriba de la de enlace de datos. Dichos protocolos también están instalados y funcionan en los nodos de la LAN, pero sus funciones *no están relacionadas con tecnologías LAN específicas.* Los protocolos de las capas de red y de transporte son necesarios para que los nodos LAN se comuniquen con las computadoras conectadas a otras LAN, cuya trayectoria debe incluir enlaces WAN. Si se requiriera garantizar las operaciones entre computadoras tan sólo dentro de los límites de una LAN, los protocolos de la capa de aplicación podrían trabajar en forma directa en la capa de enlace de datos. Empero, como dichas capacidades limitadas de comunicación no satisfacen a los usuarios, cada computadora conectada a una LAN tiene que soportar la pila de protocolos en su totalidad. Por lo tanto, uno de los protocolos de la capa de red (por ejemplo, el IP o el IPX) trabaja sobre la capa de control de enlace lógico (LLC). Además, la pila de protocolos en su totalidad, no únicamente los protocolos de la capa física y de enlace de datos, tiene que instalarse en los nodos terminales de la LAN para garantizar la compatibilidad de las aplicaciones mismas que deben funcionar de manera correcta en cualquier ambiente de red (o al menos, su operación no debe depender del tamaño de la red, ya sea ésta una LAN pequeña de un solo segmento o una red con enrutamientos de gran tamaño).

La capa de enlace de datos en las LAN se divide en dos subcapas, a menudo también llamadas capas:

- Control del enlace lógico (LLC)
- Control de acceso al medio (MAC)

Las funciones LLC suelen implementarse mediante un módulo de software apropiado del sistema operativo y las funciones MAC están implementadas en hardware (adaptador de red) y en software (controlador del adaptador de red).

Capa MAC

Las principales funciones de la capa MAC son:

- Garantizar el acceso al medio de transmisión compartido.
- Transmitir tramas entre los nodos terminales mediante la funcionalidad de los dispositivos de la capa física.

El **acceso aleatorio** es uno de los principales algoritmos utilizados para acceder al medio de transmisión. Su idea es que un nodo que desee transmitir una trama trate de enviarla sin necesidad de coordinar el uso del medio de transmisión compartido con los demás nodos de la red.

Los métodos de acceso aleatorio están *descentralizados*, pues no requieren de nodo especial que actúe como árbitro en la red. En consecuencia, el método de acceso aleatorio se caracteriza por una alta probabilidad de colisiones. Una **colisión** es un intento simultáneo de transmisión de trama por varias estaciones.[2] Como resultado de una colisión, las señales provenientes de varios transmisores se traslapan y la información contenida en todas las tramas que se transmitieron durante el periodo de colisión resulta dañada. Como las LAN usan métodos muy sencillos para codificar señales, dichas redes no pueden distinguir la señal requerida de la señal agregada, en contraste con CDMA, por ejemplo, el cual puede realizar esta función.

Existen numerosos algoritmos de acceso aleatorio que reducen la probabilidad de colisiones y mejoran de esta manera el desempeño de la red. Por ejemplo, una clase de algoritmos permite que un nodo comience la transmisión de tramas solamente al empezar un intervalo de tiempo específico, generalmente llamado ranura. Esta mejora fue sugerida por primera vez en la red ALOHA y la versión modificada de este algoritmo se conoció como ALOHA ranurado. La *transmisión de las tramas de sincronización* con los tiempos de comienzo de las ranuras ha reducido a la mitad la probabilidad de que haya colisiones en la red ALOHA ranurado, garantizando de esta forma la operación normal de la red a un coeficiente de utilización moderado de hasta 36 por ciento.

Implementar un *procedimiento de sensado de portadora* antes de comenzar la transmisión es otra forma de mejorar el acceso aleatorio. A los nodos no se les permite transmitir una trama si éstos detectan que el medio de transmisión es ocupado por la transmisión de otra trama. Esto reduce la probabilidad de colisión, aunque no elimina por completo la aparición de colisiones.

Los algoritmos de acceso aleatorio no garantizan que un nodo específico obtenga acceso al medio de transmisión compartido dentro de un intervalo determinado. Sin importar qué tan grande sea el intervalo seleccionado, la probabilidad de que el intervalo de espera se exceda siempre es mayor que cero. Además, los algoritmos de acceso aleatorio no proporcionan ninguna facilidad para el soporte de la calidad de servicio (QoS) diferenciado para los distintos tipos de tráfico. En cualquier caso, todas las tramas tienen los mismos niveles de acceso al medio de transmisión.

---

[2] Los términos *estación* y *nodo* se utilizan en este libro como sinónimos.

El **acceso determinístico** es otro método muy popular de acceder al medio de transmisión compartido. Se le designa con este nombre debido a que el tiempo de espera máximo requerido para acceder al medio de transmisión siempre se conoce con antelación.

Los algoritmos de acceso determinístico utilizan dos mecanismos: estafeta circulante y poleo.

La **estafeta circulante (Token passing)** se implementa por lo regular con base en un método *descentralizado*. Cada computadora que recibe una estafeta tiene derecho a usar el medio de transmisión compartido durante un tiempo fijo: el *intervalo de posesión de la estafeta*. La computadora transmite sus tramas durante dicho tiempo y, después de que éste ha transcurrido, dicha computadora tiene que pasar la estafeta a otra computadora. Por lo tanto, si se conoce el número de computadoras que hay en la red, el tiempo de espera máximo es igual al intervalo de posesión de la estafeta multiplicado por el número de computadoras de la red. El tiempo de espera real puede ser más corto, pues si la computadora que posee la estafeta no tiene tramas que transmitir, ésta debe esperar a que transcurra el intervalo de posesión.

La secuencia de pasar la estafeta de una computadora a otra puede definirse mediante el uso de diferentes métodos. En las redes Token Ring y FDDI ésta se define por la topología de los enlaces. Una computadora en una red de anillo tiene dos vecinos: *hacia arriba* y *hacia abajo*. Dicha computadora recibe la estafeta de su vecino hacia arriba y la pasa a su vecino de abajo. El algoritmo para pasar la estafeta puede implementarse en redes con topología diferente del anillo. Por ejemplo, la obsoleta red *Arcnet*, que ha caído en desuso, utilizaba cable coaxial compartido (como Ethernet) para conectar físicamente las computadoras y el método de estafeta circulante se usaba para acceder al medio de transmisión. La estafeta se pasaba de una computadora a otra de acuerdo con una secuencia predefinida que no dependía de las ubicaciones en las que las computadoras estaban conectadas al cable.

Los **algoritmos de poleo** se basan principalmente en el uso de un método *centralizado*. En este caso hay un nodo dedicado en la red que desempeña el papel de *árbitro* del medio de transmisión compartido.

El árbitro hace el poleo de manera periódica de otros nodos de la red y pregunta si éstos tienen tramas para transmitir. Una vez que ha reunido las solicitudes, el árbitro decide a qué nodo le otorgará el acceso al medio de transmisión compartido. Después, informa de esto al nodo seleccionado, el cual transmite su trama hacia el medio de transmisión compartido. Luego de transmitirse la trama, la fase de poleo se repite.

Un algoritmo de poleo puede estar basado también en el método *descentralizado*. En este caso, todos los nodos deben informarse entre sí de antemano acerca de sus necesidades de transmisión de tramas, utilizando el medio de transmisión compartido. Más tarde, de acuerdo con un criterio específico, cada nodo, de modo independiente a los demás, determina su posición en la cola para transmitir sus tramas. Después de esto, el nodo transmite su trama cuando le llegue su turno.

Los algoritmos de acceso determinístico difieren de los de acceso aleatorio en que operan de manera más eficaz en condiciones de alta carga de la red, donde el coeficiente de utilización es cercano a uno. Por otro lado, los algoritmos de acceso aleatorio son más eficaces cuando la carga de la red es baja. Esto se debe a que dichos algoritmos permiten que las tramas se transmitan de manera inmediata sin tener que consumir tiempo para determinar si el nodo tiene derecho a acceder al medio de transmisión.

La ventaja de los métodos de acceso al medio determinístico reside en su capacidad para establecer prioridades en el tráfico. Debido a tal cualidad, estos métodos pueden garantizar soporte de QoS.

El envío de tramas se lleva a cabo por la capa MAC, la cual abarca varias etapas que, en el caso general, no dependen del método de acceso seleccionado.

- *Formateo de tramas.* En esta etapa, los campos de las tramas están llenos de información obtenida de los protocolos de las capas superiores. Dicha información incluye las direcciones de origen y destino, los datos del usuario y el código del protocolo de las capas superiores que envía estos datos. Una vez que la trama se construye, la capa MAC calcula su suma verificadora y la coloca en el campo correspondiente.
- *Envío de tramas a través del medio de transmisión.* Una vez que la trama ha sido creada y que el nodo ha podido acceder al medio de transmisión compartido, la capa MAC pasa la trama a la capa física, la cual envía todos sus campos a través del medio de transmisión, byte por byte. El transmisor del adaptador de red lleva a cabo las funciones de la capa física. El transmisor convierte todos los bytes de la trama en una secuencia de bits, los codifica por medio de señales eléctricas y ópticas apropiadas, y luego las envía a través del medio de transmisión. Después de que las señales se han enviado a través del medio de transmisión, llegan a los receptores de los adaptadores de red conectados al medio compartido. A continuación, los receptores llevan a cabo el procedimiento inverso y convierten las señales en los bytes de la trama.
- *Recepción de las tramas.* La capa MAC de todos los nodos de red conectados al medio de transmisión compartido verifica la dirección de destino de la trama que se acaba de entregar. Si dicha dirección coincide con la del receptor, la capa MAC del nodo destino seguirá con su procesamiento; de otra forma, la trama se eliminará. Un procesamiento ulterior consiste en verificar el CRC de la trama. Si está correcto el CRC de la trama recibida, la capa MAC la pasará a la capa superior de la pila de protocolos. A su vez, si el CRC de la trama no es válido, significará que la información sufrió un daño durante su transmisión y dicha trama deberá eliminarse.

Con base en esa descripción, es evidente que Ethernet pone en práctica un modo de **transmisión de datagramas half-dúplex**.

Capa LLC

La capa LLC lleva a cabo las dos funciones siguientes:

- Administrar una interfaz hacia la capa de red, la cual se encuentre adyacente a ésta.
- Garantizar la entrega de tramas confiable con el nivel de confiabilidad predefinido.

Las *funciones de interfaz de la capa LLC* incluyen la transmisión de datos del usuario y de control entre la capa MAC y la capa de red. Cuando se transmiten datos *de arriba hacia abajo,* la capa LLC recibe el paquete (por ejemplo, un paquete IP o IPX) que contiene los datos del usuario. Además del paquete, la capa de red también transmite la dirección del nodo destino en el formato LAN apropiado. Tal dirección se utilizará para entregar el paquete dentro de la LAN. En términos de la pila de protocolos TCP/IP, este tipo de direcciones se conoce como *direcciones en hardware*. La capa LLC transmite los datos recibidos de la capa de red hacia la capa MAC para su procesamiento. Además, la capa LLC también lleva a cabo el *multiplexaje*, pues los datos recibidos de varios protocolos de la capa de red se transmiten hacia un solo protocolo de la capa MAC.

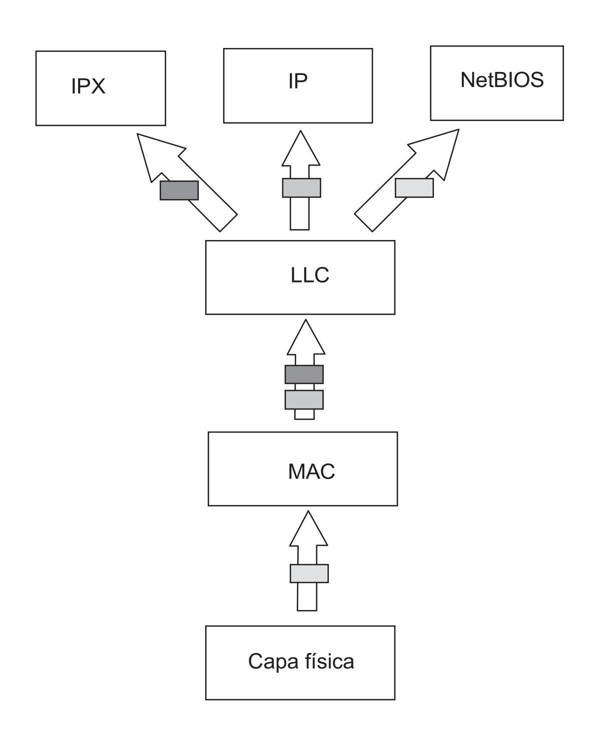


FIGURA 12.4 Demultiplexaje de tramas por el protocolo LLC.

Punto de acceso del servicio de destino (DSAP)	Punto de acceso del servicio de origen (SSAP)	Campo de control	Datos

FIGURA 12.5 Formato de trama de LLC.

Cuando se transmiten datos *de abajo hacia arriba*, la capa LLC recibe datos del usuario (por ejemplo, un paquete de la capa de red recibido desde la red) de la capa MAC. Posteriormente, ésta tiene que realizar una función de interfaz adicional, es decir, ha de decidir a qué protocolo de red deberá pasar los datos que recibió. Ésta es una *función de demultiplexaje,* ya que el flujo agregado de datos proveniente de la capa MAC deberá dividirse en varios subflujos de acuerdo con el número de protocolos de red que soporte la computadora (figura 12.4).

Las tareas de multiplexaje y demultiplexaje son características no sólo del protocolo LLC, sino también de cualquier otro protocolo sobre el cual puedan operar varios protocolos de las capas superiores. El protocolo LLC emplea campos especiales en su encabezado para el demultiplexaje de datos (figura 12.5). El **campo de acceso al servicio de destino** (**DSAP)** se utiliza para almacenar el código del protocolo al cual se envían los datos (por ejemplo, el contenido del campo *Datos*). De acuerdo con esto, el **campo punto de acceso al servicio del origen** (**SSAP**) se usa para especificar el código del protocolo, desde el cual se envían los datos. El uso de dos campos para el demultiplexaje no es típico: los protocolos por lo general pueden trabajar con un solo campo. Por ejemplo, IP suele enviar sus paquetes a IP e IPX a IPX. Dos campos son de utilidad cuando un protocolo de las capas superiores soporta varios modos de operación, de tal forma que el protocolo en el nodo emisor pueda utilizar diferentes valores de DSAP y SSAP para notificar al nodo receptor acerca del cambio a otro modo de operación. El protocolo NetBEUI a menudo sigue esta propiedad del LLC.

Considere la segunda función de la capa LLC: *garantizar la entrega confiable de tramas.* El protocolo LLC soporta varios modos de operación que difieren en la disponibilidad o falta de procedimientos para recuperar tramas en casos de pérdida o daño en ellas. Ello significa que estos modos de operación difieren en la calidad de los servicios de transporte que proporcionan. La capa LLC ubicada en forma directa adyacente a la capa de red recibe las solicitudes de la capa de red para llevar a cabo operaciones de transporte de la capa de enlace de datos caracterizadas por tener una calidad específica.

NOTA *Evidentemente, las funciones de la capa LLC que garantizan la transmisión confiable de datos en una LAN son parecidas a las de la capa de transporte del modelo OSI, aunque la capa LLC no está involucrada de manera directa en la entrega de tramas entre los nodos de la red (como lo define el protocolo de transporte). La función de entrega de tramas se delega a la capa MAC después de que ésta obtiene el acceso al medio de transmisión compartido. Sin embargo, la capa MAC lleva a cabo la entrega en el modo datagrama, lo cual significa que no establece una conexión lógica ni recupera las tramas perdidas o dañadas. Si los protocolos de las capas superiores requieren un servicio de transporte confiable, tienen que solicitarlo a la capa LLC. En este caso, la LLC establece una conexión hacia el nodo de destino y administra la retransmisión de las tramas.*

La capa LLC proporciona tres tipos de servicios de transporte a las capas superiores:

- *LLC1:* servicio no orientado a la conexión sin confirmación de la entrega. El **LLC1** proporciona al usuario las herramientas de transmisión de datos caracterizadas por una mínima cantidad de información de relleno. En este caso, el LLC soporta el modo de operación de datagrama en forma similar a MAC, de tal manera que la tecnología LAN en su totalidad trabaja en modo de datagrama. Este procedimiento se utiliza cuando la recuperación de datos después de errores y el ordenamiento de datos los llevan a cabo protocolos de las capas superiores y, por lo tanto, no necesitan estar duplicados en la capa LLC.
- *LLC2:* servicio orientado a la conexión con recuperación de tramas dañadas o perdidas. El **LLC2** brinda al usuario la habilidad para establecer una *conexión lógica* antes de comenzar a transmitir un bloque de datos. Si fuera necesario, también permite realizar procedimientos para *restablecer bloques de datos perdidos o dañados* y el ordenamiento de dichos bloques dentro de la estructura de la conexión establecida. El LLC2 usa el algoritmo de ventana deslizante para este fin.
- *LLC3: servicio no orientado a la conexión con confirmación de entrega.* En algunos casos no es deseable un tiempo de relleno para establecer una conexión lógica. No obstante, es necesario confirmar que los datos se han recibido correctamente. Un buen ejemplo de esto son los sistemas de administración en tiempo real para el control del equipo industrial. La **LLC3** adicional es proporcionada para este tipo de situaciones. Tal servicio es un compromiso entre la LLC1 y la LLC2, pues no establece una conexión, sino que confirma la recepción de los datos.

La elección del modo de operación del LLC depende de los requerimientos del protocolo de las capas superiores. La información acerca del servicio de transporte LLC necesario se envía a través de la interfaz entre capas hacia la capa LLC, junto con la dirección de hardware y los datos de usuario por medio de la interfaz de servicio entre capas.

Por ejemplo, en la pila de protocolos TCP/IP, donde la labor de garantizar la entrega confiable de datos es llevada a cabo por el protocolo TCP, la capa LLC siempre opera en el modo LLC1 y realiza operaciones sencillas, como la recuperación de paquetes de las tramas y su envío hacia uno de los protocolos de las capas superiores de la pila.

De todos los protocolos utilizados, sólo la pila de protocolo Microsoft/IBM, basada en NetBIOS/NetBEUI, emplea el modo LLC2. Esto sucede cuando el protocolo NetBIOS/NetBEUI debe operar por sí mismo en el modo que garantice la recuperación de datos perdidos o dañados. En este caso, todas estas operaciones se delegan a la capa LLC2. Si el protocolo NetBIOS/NetBEUI opera en modo datagrama, éste usa LLC1.

12.2.3 Estructura de los estándares IEEE 802.x

En 1980, el IEEE formó el Comité IEEE 802: su objetivo fue estandarizar las tecnologías LAN y la familia IEEE 802.x de estándares es el resultado de estos esfuerzos. Los estándares IEEE 802.x contienen recomendaciones acerca del diseño e implementación de las capas inferiores de las tecnologías LAN. Dichos estándares se diseñaron con base en estándares de redes propietarias de uso común, como Ethernet, Arcnet y Token Ring.

Los resultados de la labor del Comité IEEE 802 sirvieron como base para elaborar los estándares internacionales conocidos como ISO 8802-1…x. El Comité IEEE 802 es, en la actualidad, el comité internacional más importante que desarrolla estándares relacionados con la tecnología de las LAN.

En el proceso de estandarización de los protocolos de las LAN también estuvieron involucradas otras organizaciones. Por ejemplo, la ANSI diseñó el estándar FDDI para las redes que usan fibra óptica y garantiza una velocidad de transferencia de datos de 100 Mbps. Fue el primer protocolo LAN en lograr dicha velocidad, diez veces mayor que los datos de la red Ethernet clásica.

La estructura del IEEE 802 se muestra en la figura 12.6.

Arriba de la capa MAC de todas las tecnologías que se muestran en la figura 12.6 se encuentra la capa LLC, la cual es común a todas ellas e independiente de cualquier tecnología específica de LAN. El estándar LLC está administrado por el grupo de trabajo (WG) **IEEE 802.2.** Aun las tecnologías estandarizadas fuera de la estructura del Comité IEEE 802 (como el protocolo FDDI de la ANSI) se han diseñado para usar el protocolo LLC como lo define el estándar 802.2.

La descripción de cada tecnología en el estándar se divide en dos partes: la capa MAC y la capa física. Como se muestra en la figura 12.6, en prácticamente cualquier tecnología existen variantes del protocolo de la capa física, cada una de los cuales corresponde a un solo protocolo de la capa MAC. Por razones de espacio, la figura 12.6 sólo contiene Ethernet y Token Ring, pero todos estos enunciados son válidos para otras tecnologías, como Arcnet, FDDI, Fast Ethernet, Gigabit Ethernet y 10G Ethernet.

Los estándares ideados por el grupo de trabajo **IEEE 802.1** ocupan un lugar especial, ya que son comunes a todas las tecnologías. Por ejemplo, el subcomité 802.1 ha ofrecido definiciones comunes para las LAN y sus propiedades, así como para la relación entre las tres capas del modelo IEEE 802 y el modelo OSI. En la práctica, los estándares 802.1 más importantes describen la interacción entre las diferentes tecnologías, así como los estándares que brindan la base para construir redes más sofisticadas basadas en topologías típicas. Este grupo de estándares se conoce con el nombre de **estándares de interconectividad**. Dicho grupo incluye estándares muy importantes como el 802.1D, el cual describe la lógica de operación de un puente transparente o switch; el estándar 802.1H, que describe la operación de un puente traductor capaz de conectar Ethernet a FDDI o a redes Token Ring sin necesidad de un ruteador, etc. La lista de estándares diseñados por el grupo de trabajo 802.1 del IEEE sigue creciendo. Por ejemplo, en épocas recientes ideó dos estándares importantes: el 802.1Q, que define el método para construir LAN virtuales (VLAN) en redes

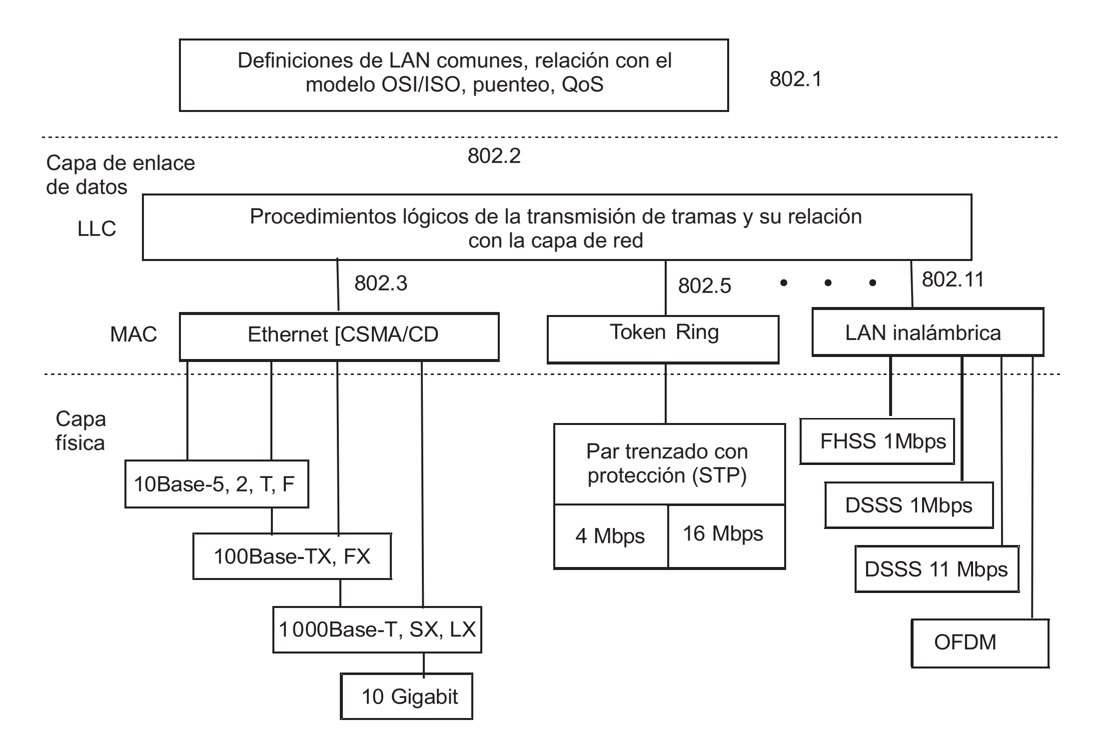


FIGURA 12.6 Estructura de los estándares IEEE 802.x.

conmutadas y el 802.1p, que describe el método para establecer prioridades de tráfico en la capa de enlace de datos (por ejemplo, garantizar el soporte de los mecanismos del QoS).

Los estándares de los grupos de trabajo **802.3**, **802.4**, **802.5** y **802.12** describen los estándares LAN, los cuales son el resultado de la mejora en las tecnologías propietarias que sirvieron como base de dichos estándares. Por ejemplo, la base del estándar 802.3 fue la Red Ethernet experimental diseñada e implementada por Xerox en 1975. En 1980, DEC, Intel y Xerox (en una alianza conocida como DIX) idearon y publicaron de manera conjunta la versión 2 del estándar Ethernet, el cual se diseñó para la red basada en cable coaxial. Esta versión de Ethernet se conoce como Ethernet DIX o Ethernet II. El estándar Ethernet DIX, a su vez, sirvió como base para desarrollar el estándar IEEE 802.3, el cual en muchos aspectos es análogo a su predecesor. El estándar 802.4 apareció como una generalización de la tecnología Arcnet ideada por Datapoint y el estándar 802.5 por lo regular cumple con la tecnología Token Ring diseñada por IBM.

El grupo de trabajo **802.11** está involucrado en el desarrollo de las LAN inalámbricas que utilizan métodos de acceso al medio de transmisión parecidos a los que usa Ethernet. Por lo tanto, los estándares 802.11 se conocen popularmente como *estándares Ethernet por radio* (aunque Ethernet no aparece en los nombres de los estándares 802.11).

Las tecnologías propietarias iniciales y sus versiones modificadas —los estándares 802.x— han coexistido por mucho tiempo. Por ejemplo, Arcnet no fue diseñada para ser compatible en su totalidad con el estándar 802.4 (y, en la actualidad es muy tarde para hacerlo, pues la producción del equipo que utiliza Arcnet salió del mercado en 1993). La única excepción es Ethernet. El último estándar propietario de Ethernet es el Ethernet DIX versión II. Desde entonces, ningún fabricante ha tratado de continuar el desarrollo de Ethernet. Todas las innovaciones de la familia Ethernet aparecieron como resultado de adoptar estándares abiertos por el Comité 802.3 del IEEE.

Estándares ulteriores fueron diseñados por grupos de compañías interesadas y, después, éstas los enviaron al grupo de trabajo IEEE 802 correspondiente para su aprobación. Éste fue el caso de tecnologías como Fast Ethernet, 100VG-AnyLAN y Gigabit Ethernet. Primero, un grupo de compañías interesadas forman una alianza a la que pueden unirse otras compañías en el desarrollo de estándares. Por lo tanto, el proceso de desarrollo de estándares era abierto por naturaleza.

12.3 CSMA/CD

PALABRAS CLAVE: dirección MAC, unidirigido, multidirigido, ampliamente dirigido, identificadores organizacionalmente únicos (OUI), acceso múltiple (MA), frecuencia de la portadora, sensado de portadora (CS), preámbulo, byte al comienzo de la trama, espacio entre paquetes (IPG), colisión, detección de colisiones (CD), secuencia de congestión, ranura de tiempo, retirada exponencial binaria truncada, valor del retardo de la trayectoria (PDV) y diámetro máximo de la red.

Las redes que se basan en Ethernet utilizan un método especial conocido como **CSMA/CD** para acceder al medio de transmisión de datos.

12.3.1 Direcciones MAC

En el nivel de la capa MAC, la cual garantiza el acceso al medio y a la transmisión de tramas, se usan direcciones únicas de 6 bytes. Tales direcciones están definidas por el estándar IEEE 802.3 y se conocen como **direcciones MAC**, las cuales en general se escriben como seis pares de dígitos hexadecimales separados por guiones o dos puntos, por ejemplo: 11-A0-17-3D-BC-01. Cada adaptador de red tiene al menos una dirección MAC.

Además de las interfaces individuales, una dirección MAC puede definir un grupo de interfaces o aun todas las interfaces de la red. El primer bit (el menos significativo) del byte más significativo de la dirección de destino indica si ésta es una dirección individual o si es de grupo. Si tal bit tiene un valor de 0, se trata de una dirección **unidirigida** (individual) que identifica a una sola interfaz de red. Si dicho bit tiene un valor de 1 se trata de una dirección **multidirigida** (de grupo). Una dirección multidirigida corresponde sólo a las interfaces configuradas (ya sea en forma manual por el administrador o de modo automático por solicitud de una capa superior) como miembros de grupos cuyo número se especifica en la dirección multidirigida. Si la interfaz de red está incluida en un grupo, entonces, de la misma forma que una dirección MAC unidirigida, tendrá otra dirección asociada con ella, llamada *dirección multidirigida*. Si una dirección multidirigida consta sólo de unos (es decir, se representa en hexadecimal como 0xFFFFFFFFFFFF), identificará a todos los nodos de la red. Dicha dirección se llama **dirección ampliamente difundida**.

El segundo bit del byte más significativo de la dirección identifica el método utilizado para asignar una dirección: **centralizado** o **local**. Si este bit tiene un valor de 0 (casi siempre éste es el caso en el equipo Ethernet estándar), la dirección habrá sido asignada de manera central de acuerdo con las reglas del IEEE 802.

NOTA *En los estándares Ethernet del IEEE, el bit menos significativo del byte es el que se encuentra en la posición más hacia la izquierda del campo y el bit más significativo ocupa la posición más hacia la derecha. Este orden de bits no estandarizado en el byte corresponde al orden en el que el transmisor de Ethernet los envía hacia la línea de*

comunicaciones (el bit menos significativo se transmite primero). Los estándares de otras organizaciones, como RFC, IETF, ITU-T e ISO, utilizan la representación de bytes tradicional en la que el bit menos significativo está en la posición más a la derecha y el bit más significativo ocupa la posición más hacia la izquierda. Al mismo tiempo, se conserva el orden de bytes tradicional. Por lo tanto, cuando se lean estándares publicados por estas organizaciones y cuando se interpreten datos desplegados en la pantalla por el sistema operativo o por un analizador de protocolos, los valores de cada byte deberán invertirse, con el fin de obtener la noción correcta de los valores de sus bits según la documentación del IEEE. Por ejemplo, cuando una dirección multidirigida es representada en notación del IEEE como 1000 0000 0000 0000 1010 0111 1111 0000 0000 0000 0000 0000 (o, lo que equivale a 80-00-A7-F0-00-00 en notación hexadecimal), muy probablemente un analizador de protocolos la desplegará en forma tradicional como 01-00-5E-0F-00-00.

El comité IEEE distribuye **identificadores organizacionalmente únicos** (**OUI**) a los fabricantes de equipo. Cada uno de estos últimos coloca el identificador asignado en los tres bytes más significativos de la dirección (por ejemplo, el 0x0020AF corresponde a 3COM y el 0x0000C a Cisco). Los fabricantes de equipo son responsables de garantizar que los tres bytes menos significativos de la dirección sean únicos. Los 24 bits reservados para los fabricantes para el direccionamiento de interfaces en sus productos permiten producir aproximadamente 16 millones de interfaces únicas con un solo identificador organizacional. La característica que tienen las direcciones distribuidas centralmente de ser únicas también opera para todas las tecnologías de LAN principales, incluidas Ethernet, Token Ring y FDDI. Las direcciones locales son asignadas por el administrador de la red, cuyas responsabilidades abarcan garantizar que estas direcciones sean únicas.

12.3.2 Acceso al medio de transmisión y transmisión de datos

Para efectos de simplicidad, cuando el lector utilice el algoritmo CSMA/CD para acceder al medio de transmisión compartido, suponga que cada nodo (estación) tiene sólo una interfaz de red.

Todas las computadoras en una red de medio compartido pueden recibir de inmediato (tomando en cuenta el retardo de propagación de la señal a través del medio de transmisión) los datos que cualquiera de las computadoras de la red comience a transmitir por el medio de transmisión compartido. El medio en el que todas las estaciones de trabajo operan en este modo se halla en el modo de **acceso múltiple (MA)**.

Para tener derecho a transmitir una trama, la interfaz emisora debe asegurarse de que el medio de transmisión compartido no esté ocupado. Esto podrá lograrse si se escucha la armónica principal de la señal, también conocida como **frecuencia de la portadora**. En consecuencia, este método se conoce como **sensado de portadora (CS)**. La principal indicación de la disponibilidad del medio de transmisión es la falta de portadora en éste. Siempre y cuando se utilice el código Manchester, el cual es adoptado por todas las variantes de Ethernet a 10 Mbps, la frecuencia de la portadora será de 5 a 10 MHz en función de la secuencia de unos y ceros que se transmita.

Si el medio de transmisión está desocupado, el nodo tendrá derecho a comenzar la transmisión de tramas. En el ejemplo que se muestra en la figura 12.7, el nodo 1 detecta que el medio de transmisión está libre y comienza a transmitir su trama. En la red Ethernet convencional basada en cable coaxial, las señales del transmisor del nodo 1 se propagan en ambas direcciones de tal forma que todos los nodos de la red reciben las tramas. Una trama de datos es acompañada siempre por un **preámbulo**, el cual está formado por 7 bytes, cada

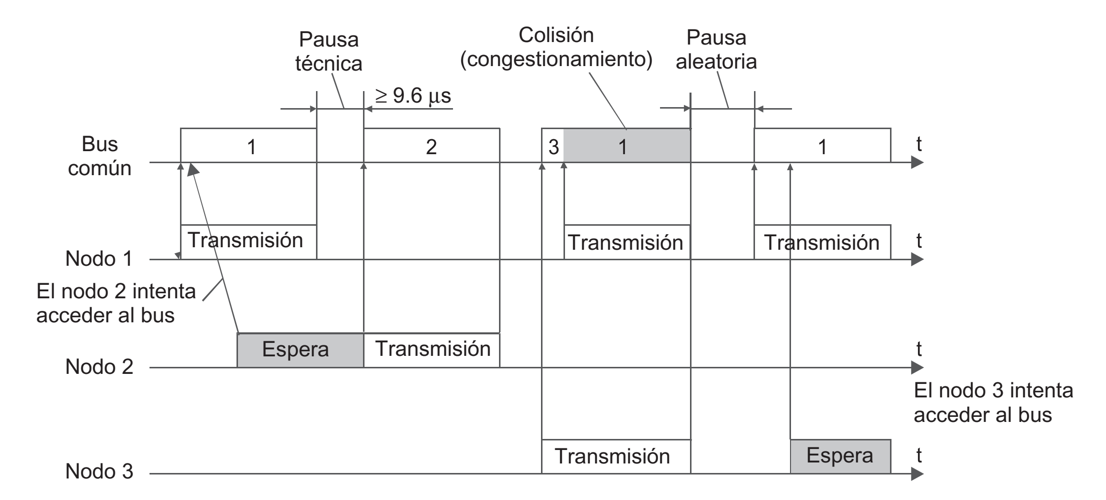


FIGURA 12.7 Método de acceso aleatorio al medio de transmisión CSMA/CD.

uno de los cuales tiene un valor de 10101010 y un octavo byte igual a 10101011. El último byte se llama **comienzo del byte de la trama**. Es necesario el preámbulo para sincronizar a nivel bit y byte entre el transmisor y el receptor. La presencia de dos unos, el segundo inmediatamente después del primero, indica al receptor que el preámbulo terminó y que el siguiente bit es el de comienzo de la trama.

Todas las estaciones conectadas al cable comienzan a almacenar los bytes de la trama que se transmite en sus memorias internas. Los primeros 6 bytes de la trama representan la dirección de destino. La estación que reconozca su propia dirección en el encabezado de trama continuará almacenando el contenido de la trama en su memoria interna y las demás estaciones dejarán de recibir la trama en esta etapa. El nodo de destino procesa los datos recibidos, los pasa hacia arriba de su pila de protocolos y después envía la trama de respuesta a través del cable. La trama Ethernet contiene la dirección de origen y la de destino; por lo tanto, el receptor sabe a dónde enviar la respuesta.

Durante la transmisión de la trama por parte del nodo 1, el nodo 2 también trata de enviar su trama. No obstante, ésta percibe que el medio de transmisión se encuentra ocupado, ya que la frecuencia de la portadora está presente. Por ende, el nodo 2 debe esperar hasta que el nodo 1 termine de transmitir su trama.

Después de que ha terminado la transmisión de tramas, todos los nodos de la red han de hacer una pausa: el **espacio entre paquetes** (**IPG**), el cual dura 9.6 µseg. Esta pausa es necesaria para regresar los adaptadores de red a sus estados iniciales, así como para evitar una situación en la que una estación monopolice el uso del medio de transmisión. Cuando ha transcurrido el IPS, los nodos de la red obtienen el derecho a comenzar la transmisión de sus tramas, ya que el medio de transmisión estará desocupado. En el ejemplo de la figura 12.7, el nodo 2 espera hasta que el nodo 1 termine la transmisión de tramas, hace una pausa de 9.6 µseg y comienza a transmitir su trama.

12.3.3 Colisiones

El sensado de portadora y el insertado de una pausa entre tramas no garantizan la eliminación de situaciones en las que dos o más estaciones decidan de manera simultánea que el medio de transmisión esté desocupado y comiencen la transmisión de sus tramas. Dicha situación se conoce con el nombre de **colisión**, pues los contenidos de las tramas

transmitidas de manera simultánea se impactan en un cable común. En consecuencia, la información de todas las tramas resulta dañada, ya que los métodos de codificación adoptados por Ethernet no permiten que las señales de cada una de las estaciones sean removidas de la señal común.

Las colisiones son normales en la operación de Ethernet. En el ejemplo que se muestra en la figura 12.8, la colisión, se origina una colisión debido a la transmisión simultánea de datos por los nodos 3 y 1. Para que se presente una colisión, no es necesario que varias estaciones comiencen a transmitir en sincronía; por el contrario, esto sucede rara vez. Es más probable que un nodo comience su transmisión de tramas y después otro nodo haga lo mismo, habiendo sensado el medio de transmisión y, al no detectar la presencia de la portadora (pues las señales del primer nodo no han llegado al segundo), empiece a transmitir su trama. Por lo tanto, las colisiones son provocadas por la ubicación distribuida de los nodos de la red.

Para manejar colisiones correctamente, todas las estaciones sensan de manera simultánea las señales en el cable. Si las señales que se transmiten y se reciben son diferentes, se registrará una **detección de colisiones (CD)**. Para aumentar la probabilidad de detección de colisiones en cuanto sea posible por todos los nodos de la red, la estación que detecta una colisión deja de transmitir su trama (en un punto cualquiera, mas no necesariamente al término de un byte) e informa de la colisión a las demás estaciones mandando una secuencia de 32 bits, conocida con el nombre de **secuencia de congestión.**

La estación que detectó la colisión debe dejar de transmitir y hacer una pausa por un intervalo aleatorio muy corto. Después de él, puede repetir su intento para utilizar el medio de transmisión y enviar la trama. La duración de las pausas de tiempo se selecciona de acuerdo con el algoritmo siguiente:

$$\text{Pausa} = L \times (\text{ranura de tiempo}) \tag{12.1}$$

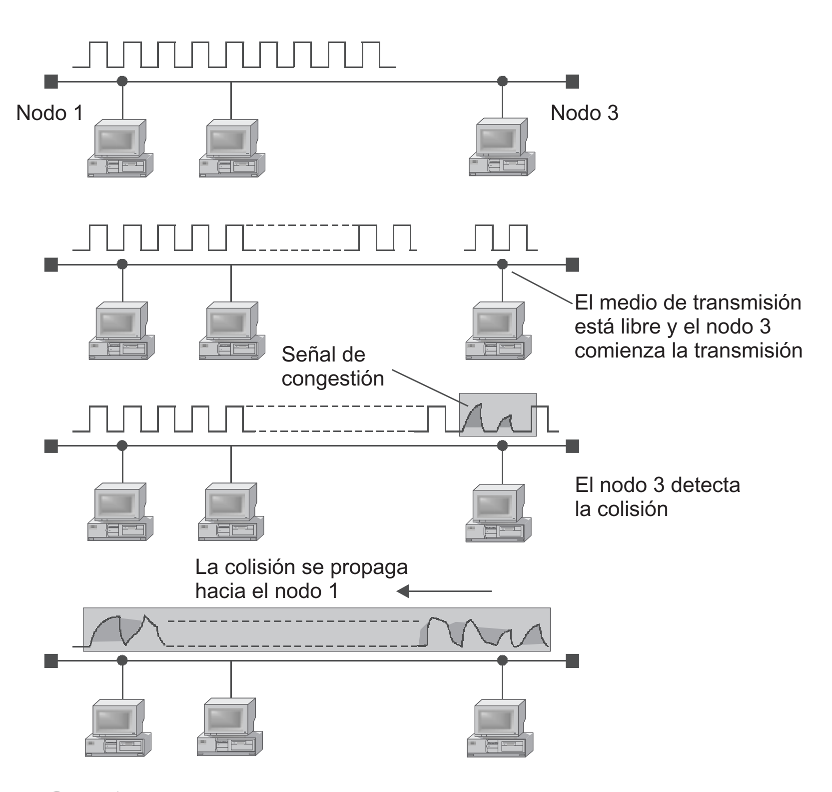


FIGURA 12.8 Origen y propagación de las colisiones.

En Ethernet, la **ranura de tiempo** se selecciona en intervalos de 512 bits (bt). El intervalo de bit corresponde al tiempo entre la aparición de dos bits secuenciales de datos en el cable. Para 10 Mbps, el intervalo de bit es de 0.1 μseg o 100 nseg.

L representa un número entero que se selecciona con igual probabilidad dentro del rango $[0, 2^N]$, donde *N* es el número de intentos repetidos para retransmitir esta trama: 1, 2,…., 10.

Después del décimo intento, el intervalo del cual se selecciona la pausa permanece constante y no se incrementa. Por lo tanto, una pausa aleatoria en la tecnología Ethernet puede tener una duración en el rango de 0 a 52.4 mseg.

Si se genera una colisión después de 16 intentos repetidos secuencialmente en la transmisión de una trama, el transmisor dejará de intentar enviar dicha trama y la eliminará. El algoritmo que se describió con anterioridad se conoce con el nombre de **retirada exponencial binaria truncada**.

El comportamiento de Ethernet en condiciones de alta carga de tráfico (cuando el coeficiente de uso del medio de transmisión crece y comienza a aproximarse a 1) corresponde por lo general a las figuras del capítulo 7 cuando se analizó el modelo M/M/1 de la teoría de colas. No obstante, el tiempo de espera antes de acceder al medio de transmisión en Ethernet comienza a crecer antes de que lo hace el modelo M/M/1: esto sucede debido a que el modelo M/M/1 es muy simple y no toma en consideración las características importantes de Ethernet como las colisiones.

Los administradores de las redes Ethernet basadas en un medio de transmisión compartido utilizan una sencilla regla empírica, de acuerdo con la cual el coeficiente de uso del medio de transmisión no debe exceder de 30%. Para soportar el tráfico sensible al tiempo, Ethernet (y otras redes basadas en un medio de transmisión compartido) puede emplear sólo un método de soporte de QoS, llamado *modo de operación de baja carga.*

12.3.4 Valor del retardo de la trayectoria y detección de colisiones

La detección confiable de colisiones por todas las estaciones de trabajo de la red es una condición necesaria para una operación correcta de la red Ethernet. Si una estación transmisora no detecta una colisión y decide que su trama de datos se transmita de manera correcta, dicha trama se perderá. Debido al traslape de señales durante condiciones de colisiones, la información contenida en la trama se dañará. Dicha trama se eliminará por la estación de trabajo receptora, debido a que la suma verificadora no coincidirá. Los datos que no fueron entregados al receptor probablemente serán retransmitidos por algunos protocolos orientados a la conexión de las capas superiores (por ejemplo, los protocolos de las capas de transporte o aplicación o el protocolo LLC, siempre que el receptor opere en el modo LLC2). A pesar de ello, la retransmisión de mensajes por los protocolos de las capas superiores se llevará a cabo mucho más tarde (a veces en varios segundos) que la retransmisión por Ethernet, el cual trabaja en intervalos de microsegundos. Por lo tanto, si las colisiones no son detectadas de modo confiable por los nodos de la red Ethernet, esto reducirá de manera significativa el ancho de banda efectivo de la red.

Para garantizar la detección confiable de colisiones se debe satisfacer la siguiente condición:

$$T_{\text{mín}} \geq \text{PDV} \tag{12.2}$$

Aquí, $T_{mín}$ es el tiempo requerido para transmitir una trama de longitud mínima y PDV significa el *valor del retardo en la trayectoria,* el cual representa el tiempo durante el cual se propaga la señal de colisión hacia el nodo más distante de la red. En el peor de los casos, la señal tiene que pasar dos veces entre los dos nodos de la red que están separados por la mayor distancia. En este caso, la señal no dañada pasa en una dirección, mientras que la señal dañada por la colisión se propaga en la dirección opuesta.

Si se satisface la condición (fórmula 12.2), la estación de trabajo transmisora deberá contar con suficiente tiempo para detectar una colisión provocada por la trama que transmitió antes de que se complete la transmisión de la trama.

La aparición de esta condición depende de la longitud mínima de la trama, la velocidad de la información del protocolo, la longitud del cable de la red y la velocidad de propagación de la señal en el cable. Dicha velocidad difiere un poco en función de los tipos de cable.

Todos los parámetros del protocolo Ethernet se seleccionan con el fin de garantizar la detección confiable de colisiones en condiciones de operación normal de los nodos de la red.

Por lo tanto, el estándar Ethernet define la longitud mínima del campo de datos como de 46 bytes, los cuales, sumados a los campos auxiliares, generan una longitud mínima de trama de 64 bytes. Esto, sumado al preámbulo, da 72 bytes o 576 bits.

De lo anterior se infiere que se pueden calcular las limitaciones de distancia entre las estaciones de trabajo. En el estándar Ethernet de 10 Mbps, el tiempo que se requiere para transmitir una trama de longitud mínima es de 575 bt. En consecuencia, el PDV debe ser menor que 57.5 μseg. La distancia que la señal debe viajar durante este tipo depende del tipo de cable: para el cable coaxial, es de aproximadamente 13 280 metros. Como durante este tiempo la señal ha de viajar dos veces a lo largo del enlace de comunicaciones, la distancia entre los dos nodos no deberá exceder de 6 635 metros. El estándar especifica una distancia bastante más corta, tomando en cuenta otras limitantes más exigentes.

Una de dichas limitantes está relacionada con la atenuación máxima permitida de la señal. Para garantizar la potencia requerida de la señal conforme ésta viaja entre los dos nodos que están separados por la mayor distancia, se selecciona una longitud máxima de un segmento continuo de cable coaxial delgado de 500 metros, considerando la atenuación que ésta introduce. Evidentemente, en un cable de 500 metros, las condiciones para detectar de manera correcta las colisiones se podrán observar con un alto grado de confiabilidad para las tramas de cualquier longitud estándar, incluida la de 72 bytes. El PDV para la sección de cable de 500 metros es de sólo 43.3 bt. Por lo tanto, es posible hacer la longitud mínima de la trama aún más pequeña. Sin embargo, los diseñadores de la tecnología no la redujeron debido a que tenían en mente redes más complejas que contuvieran varios segmentos conectados a través de repetidores.

Los repetidores incrementan la potencia de las señales transmitidas de un segmento a otro. Como resultado, la atenuación de la señal disminuye, lo cual permite que la longitud de la red pueda aumentarse de manera significativa mediante el uso de varios segmentos. En las implementaciones de Ethernet con cable coaxial, los diseñadores han limitado a *cinco* el número máximo de segmentos de red; a su vez, esto limita la longitud total de la red a 2 500 metros. Aun en dicha red multisegmentada de gran tamaño, la condición para detectar colisiones se puede observar incluso con una reserva significativa. Por ejemplo, compare la distancia de 2 500 metros obtenida con base en la máxima atenuación permitida, con la distancia máxima posible de 6 635 metros calculada según el tiempo de propagación de

la señal. No obstante, en la práctica la reserva de tiempo es mucho menor pues en las redes multisegmentadas, los mismos repetidores incluyen un retardo adicional de varias docenas de intervalos de bit en la propagación de la señal. Como es natural, también se tuvo en cuenta una pequeña reserva con el fin de compensar las desviaciones de los parámetros del cable y del repetidor.

Como resultado de considerar todos esos factores, la relación entre la longitud mínima de trama y la distancia máxima posible entre las estaciones de trabajo de la red se eligió con mucho cuidado. Dicha relación garantiza la detección confiable de colisiones. La máxima distancia entre dos nodos de la red también se conoce como **diámetro máximo de la red**. Para todos los tipos de redes Ethernet, esta distancia no debe exceder de 2 500 metros.

Con una característica mejorada en cuanto a la velocidad de transmisión de tramas de los estándares más actuales basados en el mismo método de acceso al medio CSMA/CD, como Fast Ethernet, la distancia máxima entre estaciones de la red se reduce de manera proporcional al aumento de la velocidad de transmisión: en Fast Ethernet, es de alrededor de 210 metros; en Gigabit Ethernet estaría limitada a 25 metros si no fuera por la decisión de los diseñadores de incrementar la longitud mínima del paquete.

La tabla 12.1 muestra los valores de los parámetros principales para la transmisión de tramas especificados en el IEEE 802.3. Dichos parámetros no dependen del medio de transmisión físico. Es importante observar que cada variante de medio físico de la tecnología Ethernet incluye limitaciones adicionales que a veces son más restrictivas. Dichas limitaciones deben tenerse en cuenta también y se estudiarán más adelante en este capítulo.

TABLA 12.1 Parámetros de la capa MAC de Ethernet

Parámetro	Valor
Velocidad en bits	10 Mbps
Ranura de tiempo	512 bt
Espacio entre paquetes (IPG)	9.6 µseg
Número máximo de intentos de retransmisión	16
Número máximo de crecimiento de pausas	10
Longitud de la secuencia de congestión	32 bits
Máxima longitud de trama (sin el preámbulo)	1 518 bytes
Mínima longitud de trama (sin el preámbulo)	64 bytes (512 bits)
Longitud del preámbulo	64 bits
Longitud mínima de la pausa aleatoria después de una colisión	0 bt
Longitud máxima de la pausa aleatoria después de una colisión	524 000 bt
Distancia máxima entre estaciones de trabajo	2 500 m
Número máximo de estaciones de trabajo dentro de la red	1 024

12.4 FORMATOS DE LAS TRAMAS DE ETHERNET

PALABRAS CLAVE: Ethernet DIX, Ethernet II, 802.3/LLC, 802.3/802.2, 802.2 de Novell, 802.3, 802.3 de Novell, SNAP Ethernet, delimitador de inicio de trama, preámbulo, y secuencia de verificación de trama (FCS).

El estándar Ethernet definido en el estándar IEEE 802.3 proporciona el único formato posible de trama de la capa MAC. Como la capa MAC debe incluir la trama de capa LLC descrita en el IEEE 802.2, entonces, de acuerdo con los estándares del IEEE, las redes Ethernet pueden utilizar sólo una variante de la trama de la capa de enlace de datos, cuyo encabezado es una combinación de los encabezados de las subcapas MAC y LLC.

No obstante, en la práctica, las redes Ethernet utilizan cuatro formatos de trama. El mismo tipo de trama puede tener nombres diferentes, por lo que aquí se presentan algunos de los nombres más conocidos de cada tipo de trama:

- La primera versión de la trama Ethernet —**Ethernet DIX/Ethernet II**— apareció en 1980 como resultado de los esfuerzos conjuntos de tres compañías: DEC, Intel y Xerox. La alianza de estas compañías presentó su versión propietaria del estándar Ethernet al comité IEEE 802.3 y la posicionó como un proyecto internacional de estándares.
- A pesar de lo anterior, el estándar aprobado por el grupo de trabajo 802.3 difirió de la propuesta del DIX en algunos detalles; dichas diferencias también tenían que ver con el formato de la trama. Por lo tanto, apareció la segunda variante de la trama Ethernet: **802.3/LLC (802.3/802.2** u **802.2 de Novell)**.
- La tercera variante de la trama Ethernet— **802.3 a secas/802.3 de Novell**— apareció como resultado de los esfuerzos de Novell de acelerar la operación de sus pilas de protocolos propietarias de redes Ethernet.
- Por último, existe una cuarta versión del formato de trama: **Ethernet SNAP** (SNAP quiere decir protocolo de acceso a la subred). Éste fue el resultado de las actividades del comité IEEE 802.2 encaminadas a garantizar el cumplimiento de un estándar común y la flexibilidad requerida para adicionar ciertos campos o cambiar sus objetivos en un futuro.

Las diferencias en cuanto al formato de trama pueden resultar en una incompatibilidad del hardware y software de la red diseñada para la operación con solamente un formato de trama Ethernet. Empero, en la actualidad, casi todos los adaptadores de red y sus controladores, puentes, switches o ruteadores son capaces de operar con todos los formatos de trama Ethernet utilizados. Las operaciones de reconocimiento que se requieran son llevadas a cabo de manera automática.

Los formatos de los cuatro tipos de tramas Ethernet se muestran en la figura 12.9.

12.4.1 802.3/LLC

El encabezado de la *trama 802.3/LLC* es el resultado de unir los campos de los encabezados de trama definidos por los estándares 802.3 y 802.2 del IEEE.

El estándar 802.3 define ocho campos de encabezados (el preámbulo y el delimitador de inicio de trama no se muestran en la figura 12.9):

- El *preámbulo*, que consiste en 7 bytes de sincronización que forman la secuencia siguiente: 10101010. Cuando se utiliza el código Manchester, esta combinación se representa

Trama 802.3/LLC

6	6	2	1	1	1(2)	46-1 497(1 496)	4
DA	SA	L	DSAP	SSAP	Control	Datos	FCS
			Encabezado de LLC				

Trama Raw (simple) 802.3 de Novell/802.3

6	6	2	46-1 500	4
DA	SA	L	Datos	FCS

Trama Ethernet DIX(II)

6	6	2	46-1 500	4
DA	SA	T	Datos	FCS

Trama SNAP de Ethernet

6	6	2	1	1	1	3	2	46-1 492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Datos	FCS
			AA	AA	03	000000			
			Encabezado de LLC			Encabezado de SNAP			

FIGURA 12.9 Formatos de las tramas de Ethernet.

mediante una señal de onda periódica con una frecuencia de 5 MHz en el medio de transmisión.

- El *delimitador de comienzo de la trama*, que abarca un solo byte con el patrón siguiente: 10101011. La ocurrencia de esta combinación de bits indica que el próximo byte es el primero del encabezado de trama.
- La *dirección de destino* (DA), que puede tener una longitud de 2 o 6 bytes. En la práctica, las direcciones MAC de 6 bytes siempre se utilizan.
- La *dirección de origen* (SA), que es un campo de 2 o 6 bytes que contiene la dirección MAC del emisor. El primer bit de la dirección se fija siempre a un valor cero.
- La *longitud* (L), que es un campo de 2 bytes que determina la longitud del campo de datos de la trama.
- El *campo de datos*, que puede estar formado por 0 a 1 500 bytes. Con todo, si la longitud del campo es menor que 46 bytes, el campo siguiente, de relleno, se utilizará para completar la trama a la *longitud mínima aceptable de 46 bytes.*
- El *campo de relleno*, que contiene suficientes bytes de relleno para garantizar la longitud mínima del campo de datos: 46 bytes. Esto garantiza la operación correcta del mecanismo de detección de colisiones. Si la longitud del campo de datos es suficiente, no será necesario que el campo de relleno aparezca en la trama.
- La *secuencia de verificación de trama* (FCS), que abarca 4 bytes que contienen la suma verificadora. Este valor se calcula de acuerdo con el mecanismo CRC-32.

La trama 802.3 representa la trama de la subcapa MAC; por lo tanto, según el estándar 802.2, su campo de datos encapsula la trama de la subcapa LLC con las banderas de inicio y final de trama que se quitaron. El formato de la trama LLC se describió con anterioridad. Como la trama LLC tiene una longitud de encabezado de 3 bytes (modo LLC1) o de 4 bytes (modo LLC2), el tamaño máximo del campo de datos se reduce a 1 496 o 1 497 bytes.

12.4.2 Trama 802.3/Novell 802.3

La *trama 802.3 Raw*, también conocida como *trama 802.3 de Novell*, se muestra también en la figura 12.9, en la cual se observa claramente que es la trama de la subcapa MAC de acuerdo con el estándar 802.3, sin la trama encapsulada de la subcapa LLC. Novell no utilizó los campos auxiliares de la trama LLC en su sistema operativo NetWare por mucho tiempo, ni hubo necesidad de identificar el tipo de información encapsulada en el campo de datos, pues éste siempre contenía el paquete IPX. El protocolo IPX fue durante mucho tiempo el único protocolo de capa de red en el NetWare de Novell.

Cuando fue indispensable identificar los protocolos de las capas superiores, Novell consideró la posibilidad de encapsular la trama LLC en la trama de la capa MAC (es decir, comenzó a utilizar tramas 802.3/LLC estándares). La compañía ahora designa dichas tramas como de índole 802.2 en sus sistemas operativos, aunque éstos en realidad son una combinación de los encabezados 802.3 y 802.2.

12.4.3 Trama Ethernet DIX/Ethernet II

Ethernet DIX, también conocido como *Ethernet II*, tiene una estructura que coincide con la de la trama 802.3 a secas (véase la figura 12.9). No obstante, el campo *L* de 2 bytes de la trama 802.3 a secas se utiliza como un campo de tipo de protocolo en la trama *Ethernet DIX*. Este campo, llamado *Type (T)* o *EtherType*, está diseñado para los mismos propósitos que los de los campos *DSAP* y *SSAP* de la trama del LLC, para especificar el tipo de protocolos de las capas superiores, cuyo paquete está encapsulado en el campo de datos de esta trama.

En contraste con los códigos de protocolo de los campos SAP, los cuales tienen una longitud de 1 byte, el campo *T* proporciona 2 bytes para el código de protocolo. Por lo tanto, en general, el mismo protocolo será codificado mediante valores numéricos diferentes en los campos SAP y T. Por ejemplo, IP tiene el código 2048_{10} (0x0800) para el campo *EtherType*, y en los campos SAP el mismo protocolo está codificado mediante el valor 6. Los valores de los códigos de protocolo para el campo *EtherType* aparecieron antes que los valores SAP, pues la versión propietaria de Ethernet DIX existía antes de adoptar el estándar 802.3. En consecuencia, cuando el uso del equipo que cumplía con el estándar 802.3 fue muy extendido, dichos valores constituyeron el estándar *de facto* en la mayoría de los productos de hardware y software. Puesto que las estructuras de las tramas de Ethernet DIX y 802.3 a secas coincidían, el campo *Lenght/Type* se designaba a menudo como el campo *L/T* en la documentación técnica. El número que contiene este campo determina su uso: si su valor era menor que 1 500, se trataba del campo *L*; de otra forma, era el campo *T*.

12.4.4 Trama Ethernet SNAP

Con el fin de eliminar inconsistencias en los tipos de codificación de protocolos cuyos mensajes están encapsulados en el campo datos de las tramas Ethernet, el grupo de trabajo 802.2 del IEEE se ha esforzado en estandarizar las tramas de Ethernet. Como resultado, apareció una nueva trama Ethernet: Ethernet SNAP (véase la figura 12.9), una extensión de la trama 802.3/LLC. Dicha extensión se logró mediante la inclusión de un encabezado SNAP adicional que comprende dos campos: el *OUI* y el *Type* (T). El campo T incluye 2 bytes y es una copia del campo *T* de la trama Ethernet II en cuanto a formato y propósito. Esto significa que dicho campo utiliza los mismos valores de los códigos del protocolo. A su vez, el campo *OUI* define el identificador de la organización que controla los códigos de protocolo en el campo *T*. La introducción del encabezado SNAP permitió lograr la compatibilidad con

los códigos de protocolo en la trama Ethernet II y que se creara un método universal de codificación de protocolos. Los códigos de protocolos para las tecnologías 802 están controlados por el IEEE, el cual tiene un valor de OUI de 000000. Si algunas tecnologías novedosas que probablemente aparezcan requirieran otros códigos de protocolo, será suficiente especificar otro valor de OUI para la organización que asigna dichos códigos; los valores del código antiguo permanecerán en uso (con el OUI apropiado).

Como el SNAP es un protocolo encapsulado en el protocolo LLC, los campos *DSAP* y *SSAP* contienen el código 0xAA asignado al protocolo SNAP. El campo *control* del encabezado LLC se fija a un valor de 0x03, el cual corresponde al uso de tramas no numeradas.

El encabezado SNAP es un complemento del LLC, por lo cual su uso está permitido no sólo en las tramas Ethernet, sino también en las tramas de otras tecnologías 802. Por ejemplo, el protocolo IP siempre utiliza la estructura de los encabezados LLC/SNAP en el proceso de encapsulamiento de sus paquetes en las tramas de todos los protocolos LAN: FDDI, Token Ring, 100VG-AnyLAN, Ethernet, Fast Ethernet y Gigabit Ethernet. Aun así, cuando se transmiten paquetes IP mediante el empleo de las redes Ethernet, Fast Ethernet y Gigabit Ethernet, IP usa las tramas Ethernet DIX.

12.4.5 Uso de los diferentes tipos de tramas Ethernet

Como existen cuatro tipos de tramas Ethernet, los protocolos de la capa de red deben resolver el problema de seleccionar el tipo de trama específico. Éstos deben tomar una decisión, ya sea que siempre utilicen solamente el tipo de trama, que empleen los cuatro tipos o que den preferencia sólo a los tipos de trama específicos.

El protocolo IP puede usar dos tipos de tramas: Ethernet II original o Ethernet SNAP, el cual tiene una estructura más compleja. Ethernet II es el tipo de trama preferido por el protocolo IP.

Los adaptadores de red actuales reconocen de manera automática el tipo de trama Ethernet con base en los valores de los campos de la trama. Por ejemplo, las tramas Ethernet II pueden distinguirse fácilmente de todos los demás tipos de tramas mediante el valor del campo *L/T*. Si este valor excede 1 500, significará que se trata del campo T, pues los valores de los códigos del protocolo se seleccionan de tal forma que siempre excedan 1 500. La presencia del campo *T* significa que ésta es una trama Ethernet II, la cual es la única que utiliza dicho campo en la posición de trama dada.

El protocolo IPX es el que representa lo más avanzado en este sentido, ya que puede trabajar con todos los tipos de tramas Ethernet. Dicho protocolo reconoce las tramas Ethernet utilizando el método descrito con anterioridad y, si la trama que se considera tiene otro tipo, en cuyo caso el campo *L/T* tendrá un valor menor o igual a 1 500, entonces se llevarán a cabo más verificaciones. El reconocimiento del tipo de trama se habilita mediante la presencia o ausencia de los campos LLC. Dichos campos pueden no estar presentes sólo cuando el campo *L* se halla directamente seguido por el punto de comienzo del paquete IPX, es decir, por el campo de 2 bytes. Este campo siempre está formado por unos, lo cual produce un valor de 0xFFFF o dos bytes secuenciales fijados a 255. En primera instancia, se intenta interpretar estos 2 bytes como campos *DSAP* y *SSAP*. Empero, es imposible que los campos *DSAP* y *SSAP* contengan dichos valores de manera simultánea, por lo cual la presencia de 2 bytes fijados en 255 indica que se trata de la trama 802.3 a secas.

En los demás casos, se lleva a cabo un análisis en función de los valores de los campos *DSAP* y *SSAP*. Si éstos tienen un valor 0xAA se tratará de la trama Ethernet SNAP; de otra forma, constará de la trama 802.3/LLC.

12.5 MÁXIMO DESEMPEÑO DE LA RED ETHERNET

PALABRAS CLAVE: velocidad nominal del protocolo, ancho de banda efectivo del protocolo y coeficiente de utilización de la red segmentada Ethernet.

El desempeño de la red depende de la velocidad de la transmisión de tramas a través de los enlaces de comunicaciones y de la velocidad a la que los dispositivos de comunicaciones las procesan. Cuando se procesan las tramas, dichos dispositivos las transmiten entre sus puertos, a los cuales se encuentran conectados enlaces de comunicaciones. La velocidad de transmisión de tramas por medio de enlaces de comunicaciones depende de los protocolos de las capas física y de enlace de datos que se utilicen. Por ejemplo, dichos protocolos pueden ser el Ethernet a 10 Mbps, el Ethernet a 100 Mbps, el Token Ring o el FDDI.

La velocidad a la que el protocolo transmite bits a través del enlace de comunicaciones se llama **velocidad nominal del protocolo**.

La velocidad a la que se procesan las tramas por el dispositivo de comunicaciones depende del desempeño de los procesadores de dicho dispositivo, de su arquitectura interna y de otros parámetros. Como resulta evidente, el desempeño del dispositivo de comunicaciones debe estar de acuerdo con la velocidad de transmisión del enlace. Si la velocidad del dispositivo es menor que la velocidad del enlace, las tramas sufrirán retardos en colas y se eliminarán en caso de que se sature la memoria. Por otro lado, la utilización de dispositivos de comunicaciones que trabajen a una velocidad cientos de veces mayores que la del enlace de comunicaciones tampoco tiene sentido.

Para evaluar el desempeño que requieren los dispositivos de comunicaciones equipados con puertos Ethernet, es necesario evaluar el desempeño del *segmento Ethernet.* No obstante, esta evaluación deberá realizarse no en bps (como ya es sabido, este valor es igual a 10 Mbps), sino en tramas por segundo. Esto se debe a que a un puente, un ruteador o un switch le toma aproximadamente el mismo tiempo procesar cada trama, sin considerar su longitud: el tiempo requerido para consultar la tabla de ruteo, conformar una nueva trama (con un ruteador), etc. Por otro lado, cuando la longitud de la trama tiene un valor mínimo, el número de tramas que llegan al dispositivo por unidad de tiempo alcanza un valor máximo, como es natural. En consecuencia, el modo de operación más difícil del equipo de comunicaciones incluye el **procesamiento de un flujo de tramas de longitud mínima**.

Utilice los parámetros que se proporcionan en la tabla 12.1 para calcular el máximo desempeño de los segmentos Ethernet en un número de tramas (paquetes) de longitud mínima transmitidas por segundo.

NOTA *Cuando se especifica el desempeño de la red, los términos trama y paquete se utilizan como sinónimos. De acuerdo con esto, las unidades de medida tales como tramas por segundo (fps) y paquetes por segundo (pps) también son sinónimos.*

Antes de calcular el número máximo de tramas de longitud mínima que pueden circular con un segmento Ethernet, se debe observar que el tamaño de una trama de longitud mínima más el preámbulo es de 72 bytes; 46 bytes es el tamaño mínimo del campo de datos. Por lo tanto, la longitud mínima de la trama es de 576 bytes (figura 12.10) y su transmisión requiere 57.5 µseg. Sumar el IPG (9.6 µseg) da como resultado: 67.1 µseg. *De aquí que la máxima utilización posible del segmento Ethernet es de 14 880 fps.* Como es natural, la presencia de



FIGURA 12.10 Cálculo de la utilización del protocolo Ethernet.

varios nodos dentro del segmento reduce este valor, debido tanto al tiempo que se requiere esperar hasta que se permite al nodo acceder al medio de transmisión, como a la presencia de colisiones.

Las tramas de longitud máxima en Ethernet tienen una longitud del campo de datos de 1 500 bytes. Incluida la información auxiliar, es de 1 518 bytes; con el preámbulo, el tamaño total de dicha trama es de 1 526 bytes o 12 208 bits. *La utilización máxima de un segmento Ethernet cuando procesa tramas de longitud máxima es de 813 fps.* Cuando trabaja con tramas de gran tamaño, la carga en los puentes, switches y ruteadores se reduce de manera notoria.

Ahora, calcule el ancho de banda efectivo máximo de un segmento Ethernet (medido en bits por segundo) cuando se utilizan tramas de tamaños diferentes.

> El **ancho de banda efectivo del protocolo** es la velocidad máxima de transmisión de datos del *usuario* que alcanza el campo de datos de la trama.

Este ancho de banda es siempre menor que la velocidad de bits nominal del protocolo Ethernet debido a los factores siguientes:

- Presencia de información de control en la trama.
- IPG.
- Tiempo de espera para acceder al medio de transmisión.

Para tramas de longitud mínima, el ancho de banda efectivo es:

$$B_e = 14\,880 \times 46 \times 8 = 5.48 \text{ Mbps} \qquad (12.3)$$

Este valor es de alguna forma menor que 10 Mbps, aunque se debe tomar en cuenta que las tramas de longitud mínima se utilizan fundamentalmente para transmitir confirmaciones. Por lo tanto, esta velocidad expresa sólo una relación sutil con la velocidad de transmisión de los datos del archivo.

Para tramas de longitud máxima, el ancho de banda efectivo es:

$$B_e = 813 \times 1\,500 \times 8 = 9.76 \text{ Mbps} \qquad (12.4)$$

Cuando se emplean tramas de tamaño moderado con un campo de datos de 512 bytes, el ancho de banda del protocolo es de 9.29 Mbps.

En los dos últimos casos, el ancho de banda del protocolo demuestra estar lo bastante cercano al ancho de banda máximo de 10 Mbps, aunque al realizar este cálculo se supuso que ninguna otra estación interfería con la interacción de las dos estaciones de trabajo que se comunicaban (es decir, no había colisiones ni necesidad de esperar para acceder al medio de transmisión).

> Por lo tanto, cuando no hay colisiones, el coeficiente de utilización de la red depende del tamaño de la trama del campo de datos y tiene un valor máximo igual a 0.976 cuando se transmiten tramas de longitud máxima.

12.6 ESPECIFICACIONES DEL MEDIO FÍSICO DE ETHERNET

PALABRAS CLAVE: 10Base-5, 10Base-2, 10Base-T, 10Base-f, terminador, transceptor, interfaz de la unidad de conexión (AUI), control del parloteo, detector de colisiones, elemento de desacoplamiento, la regla 5-4-3, la regla de los cuatro concentradores, conector T, concentradores, puntos de unión, Ethernet sincrónico, dominio de colisión, FOIRL, 10base-FL, 10Base-FB.

Históricamente, las primeras redes Ethernet se crearon con base en un cable coaxial con un diámetro de 12 mm. Más adelante se definieron otras especificaciones de la capa física para el estándar Ethernet que permitían usar varios medios de transmisión. El método CSMA/CD y todos los parámetros de tiempo se conservaron iguales para todas las especificaciones del medio de transmisión físico de Ethernet a 10 Mbps.

Las especificaciones físicas de Ethernet incluyen los medios de transmisión de datos que se mencionan a continuación:

- **10Base-5:** cable coaxial de 12 mm de diámetro, también llamado cable coaxial delgado. Tiene una impedancia de 50 ohms. Lo longitud máxima de un segmento es de 500 metros (sin repetidores).
- **10Base-2:** cable coaxial de 6 mm de diámetro, también conocido como cable coaxial delgado. Tiene una impedancia de 50 ohms. La longitud máxima de segmento (sin repetidores) es de 185 metros.
- **10Base-T:** cable basado en par trenzado sin protección (UTP). Forma una topología estrella basada en un concentrador central. La distancia entre el concentrador y el nodo terminal no debe exceder de 100 metros.
- **10Base-F:** cable de fibra óptica cuya topología es similar a 10Base-T. Existen varias versiones de esta especificación: e*nlace interrepetidor de fibra óptica* o FOIRL (distancias de hasta 1 000 metros), 10Base-FL (distancias de hasta 2 000 metros) y 10Base-FB (distancias de hasta 2 000 metros).

El número 10 en los nombres de la especificación significa la velocidad de transmisión de los datos de acuerdo con estos estándares: 10 Mbps. La componente base se refiere al método de codificación (banda base) cuando se usa una sola frecuencia base de 10 MHz (en contraste con los métodos que utilizan varias frecuencias portadoras, los cuales se llaman de banda ancha). El último carácter en el estándar significa el tipo de cable.

12.6.1 10Base-5

El estándar 10Base-5 corresponde generalmente a la red Ethernet experimental diseñada por Xerox y se puede considerar que es el estándar clásico de Ethernet.

La figura 12.11 muestra diversos componentes de una red basada en cable coaxial delgado formada por tres segmentos conectados mediante repetidores.

El cable se emplea como monocanal para todas las estaciones. Un segmento de cable de longitud máxima de 500 metros (sin repetidores) debe tener **terminadores** de 50 ohms conectados en ambos extremos. Los terminadores están diseñados para absorber las señales que se propagan a través del cable de tal forma que no se reflejen hacia atrás. Si no se colocan dichos terminadores, surgen ondas estacionarias en el cable; por lo tanto, algunos nodos reciben señales poderosas y las señales entregadas a los demás nodos son tan débiles que resulta imposible recibirlas.

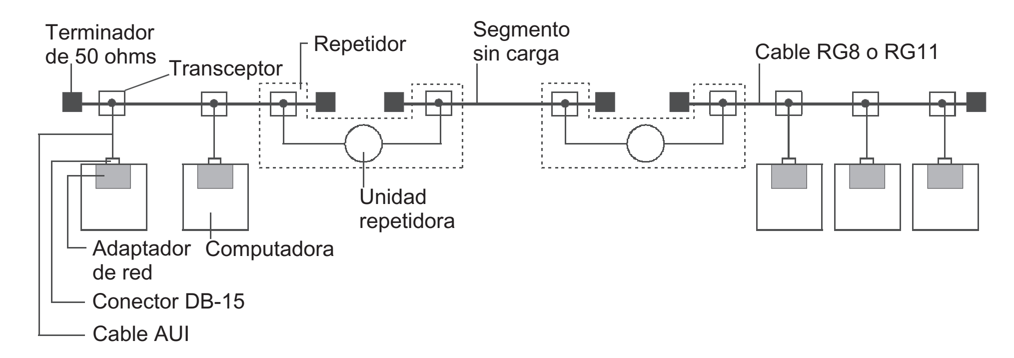


FIGURA 12.11 Componentes de la capa física de una red 10Base-5 formada por tres segmentos.

Una estación de trabajo se conecta al cable mediante el uso de un **transceptor**: a parte del adaptador de red, lleva a cabo las funciones de transmisión y recepción (**tran**smisor + **rece**ptor = transceptor). El transceptor está conectado directamente al cable y alimentado del adaptador de red instalado en la computadora. El transceptor puede estar conectado al cable mediante una conexión que penetre el cable y garantice el contacto físico directo con el cable (conexión tipo vampiro) o por algún método en el que no se haga contacto físico.

Un transceptor se conecta al adaptador de red mediante el uso del cable de interfaz de la **unidad de interfaz de conexión (AUI)**, el cual puede ser de hasta 50 metros. El AUI abarca cuatro pares trenzados (el adaptador de red debe contar con un conector AUI). La presencia de una interfaz estándar entre el transceptor y la parte sobrante del adaptador de red es muy útil cuando se trata de migrar de un tipo de cable a otro. Para tal propósito, es suficiente reemplazar el transceptor; la parte que queda del adaptador de red no necesita reemplazarse, pues ésta implementa el protocolo de la capa MAC. En este caso, sólo es necesario asegurarse de que el nuevo transceptor (por ejemplo, el transceptor para par trenzado) soporte el estándar AUI.

No pueden estar conectados a un solo segmento más de 100 transceptores y la distancia entre los puntos de conexión de los transceptores no debe ser menor que 2.5 metros. El cable cuenta con marcas cada 2.5 metros que indican los puntos de conexión de los transceptores. Cuando las computadoras se conectan de acuerdo con dichas marcas, la influencia de ondas estacionarias en el cable de los adaptadores de red se reduce al mínimo.

La figura 12.12 muestra la estructura simplificada de un transceptor. El transmisor y el receptor se conectan al mismo punto del cable mediante el uso de un circuito especial (por ejemplo, un transformador) que permite administrar transmisiones y recepciones simultáneas de señales hacia el cable y desde él.

En caso de que el adaptador no funcione bien, puede ocurrir que una secuencia de señales arbitrarias circule continuamente por el cable. Debido a que el cable es un medio de transmisión compartido por todas las estaciones de trabajo, el mal funcionamiento de un solo adaptador bloqueará la operación de la red. Para evitar dicha situación, la salida del transceptor cuenta con un esquema especial que verifica el tiempo de transmisión de las tramas. Si el tiempo máximo posible de la transmisión de tramas se excede (proporcionando algún tiempo se reserva), el esquema simplemente desconectará la salida del transmisor del cable. El tiempo máximo de transmisión de tramas (incluido el preámbulo) es de 1 221 μseg y el límite de transmisión de tramas es de 4 000 μseg (4 mseg). Esta función del transceptor se conoce a menudo con el nombre de *control del parloteo.*

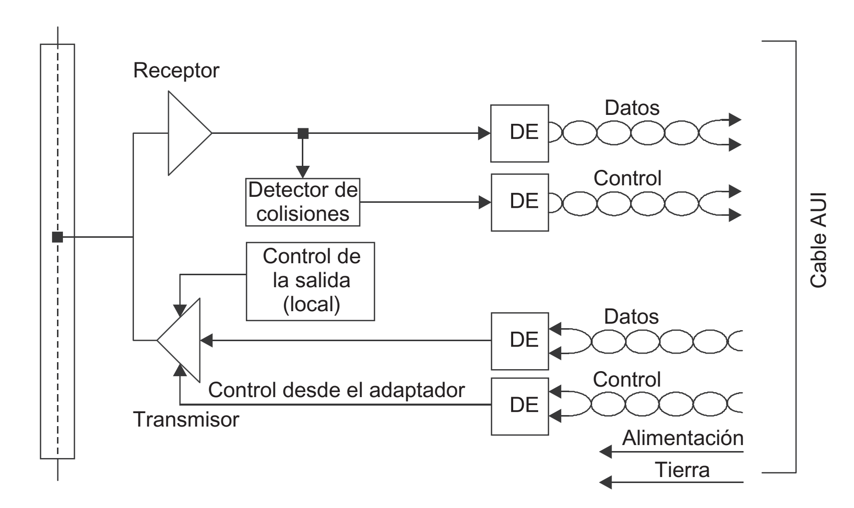


FIGURA 12.12 Diseño estructural de un transceptor.

El **detector de colisiones** detecta la presencia de colisiones en el cable coaxial mediante el aumento del nivel de la componente constante de la señal. Si dicha componente constante excede un valor de umbral específico (alrededor de 1.5 V), significará que al menos dos transmisores envían señales por el cable de manera simultánea.

Los **elementos de desacoplamiento** garantizan el desacoplamiento galvánico del transceptor respecto a la parte sobrante del adaptador de red, protegiendo de esta manera al adaptador y a la computadora de las abruptas caídas de tensión que pudieran surgir del cable dañado.

10Base-5 determina la posibilidad de utilizar un dispositivo conocido con el nombre de repetidor. Éste conecta varios segmentos de cable y forma una sola red, con lo cual incrementa su longitud total. El repetidor recibe señales provenientes del segmento de cable y, de manera sincronizada, las repite bit por bit hacia otro segmento, de tal modo que mejora las formas de las mismas, incrementa su potencia y sincroniza los pulsos. Un repetidor abarca dos (o más) transceptores conectados a segmentos de cable, así como a una unidad repetidora con su propio oscilador de reloj. Para obtener una mejor sincronización, el repetidor retarda la transmisión de los primeros bits del preámbulo de las tramas, de tal manera que incrementa el retardo de transmisión de tramas de un segmento a otro y reduce ligeramente el IPG.

El estándar permite a no más de cuatro repetidores en la red y, en consecuencia, a no más de cinco segmentos de cable. Dada la longitud máxima de un segmento de cable (500 metros), esto da una longitud máxima de 2 500 metros en el caso de una red 10Base-5. Ello corresponde exactamente a la limitante general acerca del diámetro máximo de la red para Ethernet.

Sólo tres de los cinco segmentos pueden estar congestionados (es decir, pueden tener nodos terminales conectados a ellos). Los segmentos congestionados deben separarse de los no congestionados, de tal forma que la máxima configuración de red incluya dos segmentos congestionados conectados por segmentos no congestionados a un segmento congestionado central. En la figura 12.11 se mostró un ejemplo de una red Ethernet formada por tres segmentos conectados mediante dos repetidores. Los segmentos de los extremos estaban congestionados, mientras que el intermedio no lo estaba.

La regla de acuerdo con la cual los repetidores se utilizan en la red Ethernet 10Base-5 se conoce como **regla 5-4-3**: cinco segmentos, cuatro repetidores y tres segmentos congestionados.

El número limitado de repetidores se explica mediante los retardos de propagación adicionales de las señales que introducen los repetidores. El uso de repetidores aumenta el PDV, el cual con una detección confiable de colisiones no debe exceder el tiempo requerido para transmitir una trama de longitud máxima (es decir, una que tenga 72 bytes o 576 bits).

Cada repetidor está conectado al segmento mediante su propio transceptor, por lo cual no más de 99 nodos, no 100, pueden estar conectados al segmento congestionado. En consecuencia, el número máximo de nodos terminales en una red 10Base-5 es de $99 \times 3 = 297$ nodos.

12.6.2 10Base-2

El estándar 10Base-2 utiliza cable coaxial con un alambre central de cobre de 0.89 mm de diámetro y un diámetro exterior de alrededor de 5 mm (Ethernet delgado) como medio de transmisión. La impedancia del cable es de 50 ohms. La longitud máxima del segmento sin repetidores es de 185 metros; se deben conectar terminadores con una resistencia de 50 ohms a los nodos extremos del segmento. El cable coaxial delgado es más barato que el esbelto, por lo que las redes 10Base-2 a menudo se llaman redes Cheapernet. A pesar de ello, el bajo costo tiene su desventaja, ya que el cable coaxial delgado es menos inmune al ruido, tiene menor resistencia mecánica y se caracteriza por un ancho de banda menor.

Las estaciones de trabajo están conectadas al cable mediante un **conector** BNC **tipo T**, el cual es una unión T, una ramificación a la cual se conecta al adaptador de red, mientras que otras dos ramificaciones se encuentran conectadas al cable. El número máximo de estaciones de trabajo que pueden conectarse a un solo segmento es 30. La distancia mínima entre estaciones de trabajo es de un metro. El cable coaxial delgado cuenta con marcas para conectar nodos terminales espaciados un metro de distancia uno del otro.

El estándar 10Base-2 también permite usar repetidores de acuerdo con la regla 5-4-3.

En este caso, la red tendrá una longitud máxima de $5 \times 185 = 925$ metros. Como es evidente, esto es más estricto que la limitación normal de 2 500 metros.

NOTA *Se deben tener en cuenta muchas restricciones cuando se construya una red Ethernet que trabaje correctamente. Algunas de estas restricciones están relacionadas con los parámetros de la red, como la longitud máxima de la red o el número mínimo de computadoras, las cuales deben satisfacer de manera simultánea varias condiciones. Una red Ethernet instalada de manera adecuada, debe satisfacer todos los requisitos. Empero, en la práctica es suficiente con observar sólo los más estrictos. Por ejemplo, la limitante general establece que la red Ethernet debe contener no más de 1 024 nodos y que el estándar 10base-2 limita el número máximo de estaciones de trabajo conectadas a un solo segmento a 30. Como el número de segmentos congestionados está limitado a tres, el número total de nodos en una red 10Base-2 no debe exceder de $29 \times 3 = 87$.*

El estándar 10base-2 es similar al 10Base-5. A pesar de ello, en el 10Base-2 los transceptores están integrados a los adaptadores de red, pues el cable coaxial delgado más flexible puede enrutarse directamente hacia el conector BNC tipo T integrado en la parte trasera de la tarjeta de interfaz de red instalada dentro de una computadora. En este caso, el cable cuelga del adaptador de la red, lo cual hace más complicado el movimiento físico de las computadoras.

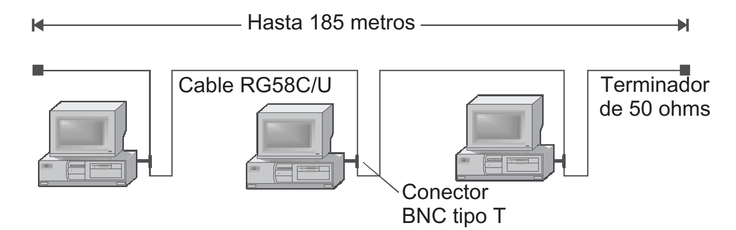


FIGURA 12.13 Red 10Base-2 estándar.

La figura 12.13 muestra una red típica fundamentada en el estándar 10base-2, que incluye un solo segmento de cable.

La implementación práctica de dicho estándar es la solución más simple para las redes que utilizan cable, porque sólo se necesitan adaptadores de red, conectores T y terminadores de 50 ohms para conectar computadoras a la red. Empero, este tipo de conexión de cable es el más vulnerable a fallas: el cable Ethernet delgado es más sensible al ruido que el cable coaxial esbelto, el monocanal tiene un gran número de conexiones mecánicas (cada conector T proporciona tres conexiones mecánicas, de las cuales dos son de vital importancia para el funcionamiento de toda la red), y los usuarios tienen acceso a los conectores y pueden dañar la integridad del monocanal. Además, esta solución está muy lejos de ser perfecta en términos de estética y ergonomía, pues dos piezas de cable muy notorias se conectan a cada estación mediante el uso de un conector tipo T. Por debajo de la mesa, a menudo se forma una bola de cables, porque es necesario proporcionar alguna reserva en caso de que se mueva ligeramente el espacio de trabajo.

Una desventaja muy común de los estándares 10Base-5 y 10Base-2 es la falta de información en línea acerca del estado del monocanal. Cualquier falla en el cable es detectada de inmediato, en virtud de que la red deja de operar en ese momento; con todo, se requiere un dispositivo especial llamado probador de cables con el fin de encontrar la sección del cable donde se presentó la falla.

12.6.3 10Base-T

Las redes 10Base-T utilizan dos UTP como medio de transmisión. El cable multipar basado en el UTP categoría 3 lo emplean compañías telefónicas por largo tiempo para conectar aparatos telefónicos dentro de edificios. Este cable también tiene un nombre —Grado de voz— que significa que se diseñó principalmente para transmitir la voz.

La idea de instalar este cable tan popular en LAN de edificios demostró dar muchos frutos, pues la mayoría de los edificios estaban provistos del sistema de cableado requerido. Solamente faltaba diseñar un método para conectar adaptadores de red y otros equipos de comunicaciones con par trenzado, de tal manera que se minimizaran los cambios en los adaptadores de red y en el software de comunicaciones de los sistemas operativos de red en comparación con la red Ethernet que utiliza cable coaxial. Este problema se resolvió con mucho éxito: cambiar a par trenzado requirió sólo cambiar el transceptor del adaptador de red o puerto del ruteador; el método de acceso y todos los protocolos de la capa de enlace de datos permanecieron iguales que en la red Ethernet con cable coaxial.

Para conectar nodos terminales a un dispositivo especial llamado repetidor multipuerto se utilizan dos pares trenzados, de acuerdo con la topología "punto a punto". Se necesita un par trenzado para la transmisión de datos desde la estación hasta el repetidor (a la salida T_x del adaptador de red) y se requiere otro para la transmisión de datos desde el repetidor hasta

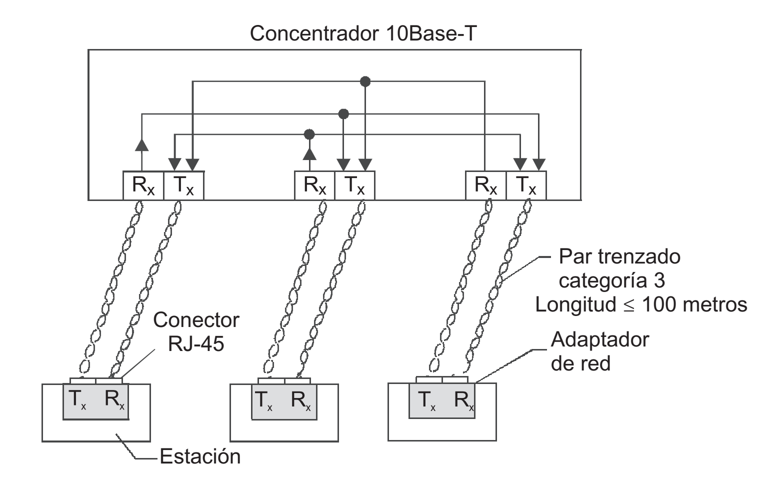


FIGURA 12.14 Red estándar 10Base-T: T_X es el transmisor y R_X el receptor.

la estación (a la entrada R_x del adaptador de red). La figura 12.14 muestra un ejemplo de un repetidor de tres puertos. El repetidor recibe las señales de uno de los nodos terminales y los transmite de manera sincrónica hacia los demás puertos, excepto a aquel desde el cual fueron recibidas las señales.

Los repetidores multipuerto en este caso se llaman **concentradores** o **puntos de unión** en lenguaje técnico. El concentrador lleva a cabo las funciones de un repetidor de señales de todas las secciones de par trenzado conectadas a sus puertos, de tal forma que crean un medio de transmisión de datos común: un monocanal lógico (o bus común lógico). El concentrador detecta las colisiones en el segmento en caso de transmisiones simultáneas de señales a través de más de una de sus entradas R_x. En este caso, el concentrador envía la secuencia de congestión a todas sus salidas T_x. El estándar define una velocidad de transmisión de datos de 10 Mbps y una longitud máxima de sección de par trenzado entre dos nodos conectados directamente (estaciones o concentradores) de no más de 100 metros, siempre y cuando se utilice un par trenzado de categoría 3 o uno mejor. Esta distancia se define por el ancho de banda del par trenzado, el cual permite transmitir datos a 10 Mbps a través de una distancia de 100 metros con el empleo del Código Manchester.

Los concentradores 10Base-T pueden conectarse entre sí mediante el uso de los mismos puertos que los diseñados para conectar nodos terminales. Cuando se procede de esta forma, es necesario asegurarse de que el transmisor y el receptor de un puerto se encuentren conectados con el receptor y el transmisor de otro puerto, respectivamente.

> El estándar 10Base-T establece el número máximo de concentradores entre cualquier par de estaciones de trabajo de la red a cuatro. Esto se conoce como **regla de los cuatro concentradores**.

La regla de los cuatro concentradores reemplaza a la *5-4-3,* aplicable a las redes que utilizan cable coaxial. Dicha regla se ideó con el fin de garantizar la sincronización entre las estaciones de trabajo cuando se ponen en práctica procedimientos de acceso CSMA/CD y para garantizar la detección confiable de colisiones.

Cuando se instalan redes 10Base-T con un gran número de estaciones de trabajo, se podrán interconectar concentradores si se utiliza el método jerárquico y, por ende, si se forma una estructura en árbol (figura 12.15).

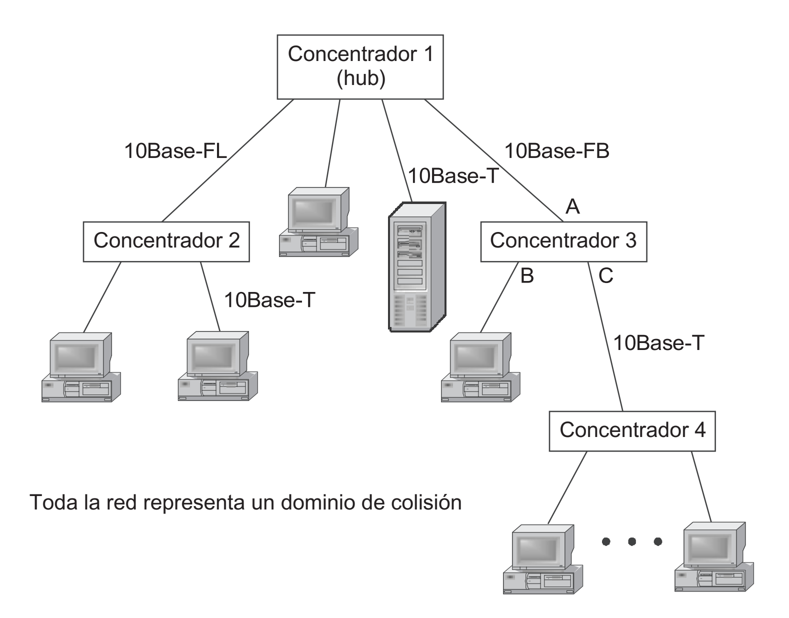


FIGURA 12.15 Conexión jerárquica de concentradores Ethernet.

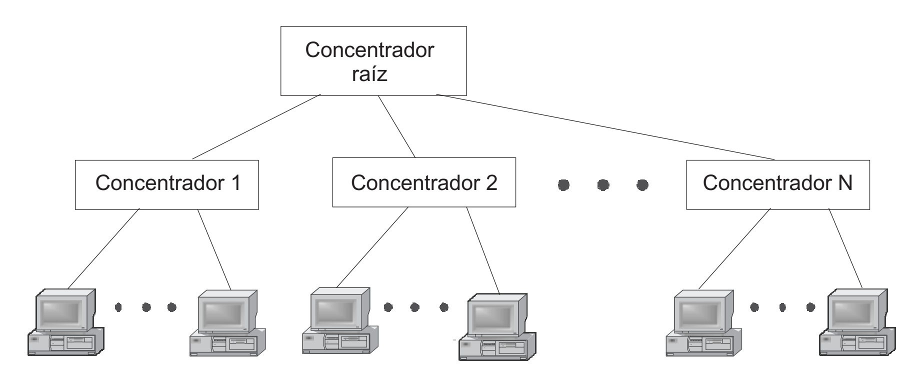


FIGURA 12.16 Sistema con el número máximo de estaciones de trabajo

NOTA *La conexión de concentradores en loop no está permitida por el estándar 10Base-T, porque resulta en una operación incorrecta de la red. Este requerimiento significa que no se permite instalar enlaces paralelos entre los concentradores que tienen una importancia crítica en las redes 10Base-T. Los enlaces paralelos son necesarios para la reservación de enlaces en caso de falla de un puerto, de un concentrador o de un cable. La reservación del enlace en una red 10Base-T será factible sólo si se conmuta uno de los enlaces en paralelo al estado de bloqueo (inactivo).*

El número total de estaciones de trabajo en la red 10Base-T no debe exceder del límite normal de 1 024. Para este tipo de capa física, dicho límite se puede alcanzar: es suficiente con crear una jerarquía de dos niveles de concentradores, colocando suficientes concentradores con 1 024 puertos totales en el nivel más inferior (figura 12.16). Los nodos terminales deben estar conectados a los puertos de los concentradores del nivel más inferior. La regla de los cuatro concentradores se satisface en este caso, porque entre cualquier par de nodos terminales habrá tres concentradores.

Debido a que no debe haber más de cuatro repetidores entre cualquier par de nodos de la red, es evidente que *el diámetro máximo de la red en el caso de las redes 10Base-T es de 5 × 100 = 500 metros.* Observe que esta limitante es más estricta que en las redes Ethernet, la cual es de 2 500 metros.

Las redes diseñadas con apoyo en el estándar 10Base-T tienen muchas ventajas respecto a Ethernet por cable coaxial debido a la división del cable físico común en secciones independientes de cable conectadas a un dispositivo central de comunicaciones. A pesar de que, desde el punto de vista lógico, dichas secciones aún forman un medio de transmisión compartido, su separación física significa que pueden ser controladas y desconectadas de manera independiente en caso de una falla en el adaptador de red, un cortocircuito o fallas en el funcionamiento de la red. Esta circunstancia simplifica de manera significativa los procedimientos de mantenimiento de las redes Ethernet de gran tamaño, porque los concentradores generalmente llevan a cabo dichas operaciones de modo automático y notifican al administrador de la red acerca de cualquier problema existente.

El estándar 10Base-T define el procedimiento para probar la operación de dos secciones de par trenzado que conectan al transceptor del nodo terminal y al puerto del repetidor. Este procedimiento, conocido como *prueba de integridad del enlace,* se basa en la transmisión de señales especiales (J y K en el Código Manchester) entre el transmisor y el receptor de cada par trenzado en intervalos de 16 mseg. Las señales de información del Código Manchester siempre cambian de voltaje en la mitad de un pulso de reloj; J y K violan esta regla, pero conservan el voltaje a la mitad de un pulso de reloj. Uno de los dos valores de voltaje corresponde al código J y otro al código K. Como J y K no son válidos durante la transmisión de la trama, la secuencia de prueba no ejerce ninguna influencia en la operación del algoritmo de acceso al medio de transmisión.

> La inclusión de cualquier dispositivo activo entre nodos terminales capaz de controlar su operación y de aislar de la red los nodos que no trabajan de manera adecuada constituye la *ventaja principal* de las redes que trabajan con la tecnología 10Base-T sobre cable coaxial, cuyo mantenimiento suele ser complicado. Gracias a la presencia de concentradores, Ethernet ha ganado algunas capacidades básicas de tolerancia a fallas.

12.6.4 Ethernet por fibra óptica

La red 10Base-F utiliza cable de fibra óptica como medio de transmisión compartido. Los estándares de fibra óptica recomiendan fibra óptica multimodo relativamente barata como el tipo de cable principal. Esta fibra tiene un ancho de banda de 500 a 800 MHz en una longitud de cable de 1 km También es aceptable la fibra óptica monomodo más costosa con un ancho de banda de varios gigahertz, aunque en este caso es necesario utilizar un tipo de transceptor especial.

Desde el punto de vista funcional, la red Ethernet basada en cable de fibra óptica está formada por los mismos elementos que el estándar 10Base-T, es decir, adaptadores de red, repetidores multipuestos y secciones de cable que conectan los adaptadores con los puertos de repetidores. Como en el caso del par trenzado se utilizan dos fibras ópticas para conectar adaptadores a los repetidores: una fibra conecta la salida T_X del adaptador a la entrada R_X del repetidor, y otra conecta la entrada R_X del adaptador a la salida T_X del repetidor.

El estándar **FOIRL** (**enlace interrepetidor por fibra óptica**) fue el primer estándar del comité IEEE 802.3 que utilizó fibra óptica en Ethernet. Este estándar garantiza la longitud del enlace de fibra óptica entre repetidores de 1 km, siempre y cuando la longitud total de la

red no exceda de 2 500 m. El número máximo de repetidores entre cualquier par de nodos de la red es 4. En este caso, el diámetro máximo de 2 500 m se puede alcanzar, aunque no se permite la longitud máxima de las secciones de cable entre los *cuatro* repetidores, como tampoco entre repetidores y nodos terminales; de otra forma, la red resultante sería de 5 000 metros.

El estándar **10Base-FL** es una mejora menor del FOIRL. La potencia de los transmisores se incrementó, por lo que la distancia máxima entre el nodo terminal y el concentrador aumentó a 2 000 metros. El número máximo de repetidores entre nodos permaneció igual en 4, mientras que la longitud máxima de la red es de 2 500 metros.

El estándar **10Base-FB** está diseñado solamente para conectar repetidores. Los nodos terminales no pueden utilizar este estándar para conectarse a los puertos del concentrador. Hasta cinco repetidores 10Base-FB pueden instalarse entre los nodos de red, en tanto que la longitud máxima de un solo segmento es de 2 000 m y la longitud máxima de la red es de 2 740 metros.

Cuando los repetidores conectados de acuerdo con el estándar 10Base-FB no tienen tramas que enviar, éstos intercambian constantemente secuencias de señales especiales diferentes de las señales de tramas de datos, lo cual se lleva a cabo para establecer la sincronía. Por lo tanto, dichas señales introducen pequeños retardos cuando se transfieren datos de un segmento a otro. Por ello, el número de repetidores permitidos se eleva a 5. Los códigos J y K de Manchester se utilizan como señales especiales en la secuencia siguiente: J-J-K-K-J-J-…. Esta secuencia genera pulsos de 2.5 MHz, de tal manera que sincroniza el receptor de un concentrador con el transmisor de otro. Por lo tanto, el estándar 10base-FB también se conoce con el nombre de **Ethernet sincrónico**.

Como en el caso del estándar 10Base-T, los estándares de Ethernet por fibra óptica permiten conectar concentradores en estructuras de árbol jerárquico solamente; empero, está prohibido instalar loops entre los puertos de un concentrador.

Al comienzo de este capítulo, el estándar 10Base-F se utilizó como término genérico para nombrar a los tres estándares Ethernet por fibra óptica a 10 Mbps. Aunque éste no es el término estándar, los especialistas en redes lo utilizan a menudo como sobrenombre.

12.6.5 Dominio de colisión

El **dominio de colisión** es parte de la red Ethernet en el sentido de que todos los nodos detectan una colisión independientemente del punto en la red donde ésta se presentó.

Las redes Ethernet construidas con base en repetidores siempre forman un dominio de colisión. Los puentes, switches y ruteadores dividen a la red Ethernet en varios dominios de colisión.

La red que se muestra en la figura 12.15 es un único dominio de colisión. Por ejemplo, si una colisión de tramas se presenta en el concentrador 4, entonces de acuerdo con la lógica de operación de los concentradores 10Base-T, la señal de colisión se propagará a todos los puertos de todos los concentradores.

Por otro lado, si el concentrador 3 se reemplaza por un puente, entonces su puerto C, conectado al concentrador 4, recibirá la señal de colisión, pero no la transmitirá a los demás puertos, pues esta función se encuentra más allá de sus responsabilidades. El puente simplemente manejará la situación de colisión al utilizar el puerto C, el cual está conectado al medio de transmisión compartido donde se presentó la colisión. Si la colisión sucedió debido a que el *puente* intentó transmitir una trama, vía el puerto C, hacia el concentrador 4, entonces

una vez que haya registrado la señal de colisión, el puerto C dejará de transmitir tramas e intentará retransmitirlas después de un intervalo aleatorio. Si el puerto C recibía una trama en el momento de la colisión, simplemente eliminará el fragmento recibido y esperará hasta que el nodo que ha transmitido la trama vía el concentrador 4 reintente la transmisión de la trama. Después de recibir con éxito esta trama en su memoria, el puente lo transmitirá a otro puerto (por ejemplo, al puerto A), como lo indique la tabla de enrutamiento. Todos los eventos relacionados con el manejo de colisiones por parte del puerto C serán una incógnita para los demás segmentos de la red conectados a otros puertos del puente.

12.6.6 Características comunes de los estándares Ethernet a 10 Mbps

Las tablas 12.2 y 12.3 resumen las limitaciones y características principales de los estándares Ethernet a 10 Mbps.

TABLA 12.2 Limitaciones comunes a todos los estándares de Ethernet

Característica	Valor
Ancho de banda nominal	10 Mbps
Número máximo de estaciones de trabajo dentro de la red	1 024
Distancia máxima entre nodos de la red	252 500 m (2 750 metros para la red 10Base-FB)
Número máximo de segmentos de cable coaxial en la red	5

TABLA 12.3 Parámetros de las especificaciones de la capa física de Ethernet

Parámetro	10Base-5	10Base-2	10Base-T	10Base-F
Cable	Cable coaxial grueso RG-8 o RG-11	Cable coaxial delgado RG-58	UTP categoría 3, 4 o 5	Cable de fibra óptica multimodo
Longitud máxima del segmento (m)	500	185	100	2 000
Máxima distancia entre nodos de la red (cuando se utilizan repetidores) (m)	2 500	925	500	2 500 (2 740 para 10Base-FB)
Número máximo de estaciones de trabajo en un segmento	100	30	1 024	1 024
Número máximo de repetidores entre dos estaciones de trabajo	4	4	4	4 (5 para 10Base-BF)

12.7 ESTUDIO DE UN CASO

A principios de la década de 1990, la planta de ingeniería Transmash utilizó una red Ethernet a 10 Mbps con un medio de transmisión compartido para interconectar todas sus minicomputadoras y sus PC (figura 12.17). Las computadoras se utilizaban principalmente para llevar a cabo tareas autónomas y el intercambio de datos entre éstas era bastante esporádico. La red transmitía pequeños volúmenes de datos alfanuméricos, por lo que un medio de transmisión compartido era suficiente para satisfacer sus necesidades de producción. Las redes de fibra óptica fundamentadas en los estándares 10Base-FB y 10Base-FL se utilizaron para conectar al segmento central de la red con segmentos de las fábricas remotas. La red cumplió con todos los requerimientos de la configuración Ethernet de multisegmentos: las secciones de cable no excedieron la longitud máxima permitida, no había más de cuatro concentradores entre cualquier par de nodos y la distancia máxima entre los nodos de red no excedía de 1 800 metros (computadoras A y C de la figura 12.17).

Después de cierto tiempo, fue necesario conectar otro edificio, el 4, a la red. Este edificio estaba ubicado dentro del rango requerido para conectarlo a la red al utilizar los estándares Ethernet por fibra óptica (10Base-FB o 10Base-FL). A pesar de ello dicha conexión podría generar una configuración incorrecta, debido a que habría cinco concentradores entre computadoras ubicadas en los edificios 1 y 4. Además, el diámetro de la red llegaría a ser de 2 800 m, lo cual representaría otra violación de las limitaciones de Ethernet. No obstante, en esas fechas el arquitecto de la red de Transmash no quería cambiar radicalmente la estructura de la red e instalar un puente o un ruteador para conectar un nuevo segmento. Él sabía que la sección 13 del estándar IEEE 802.3 titulado "Consideraciones a nivel sistema de las redes bandabase a 10 Mbps multisegmentadas" proporcionaba un procedimiento para evaluar la configuración correcta de la red. Esta técnica hace posible determinar numéricamente si una configuración específica de red trabajará de manera correcta. Los cálculos muestran

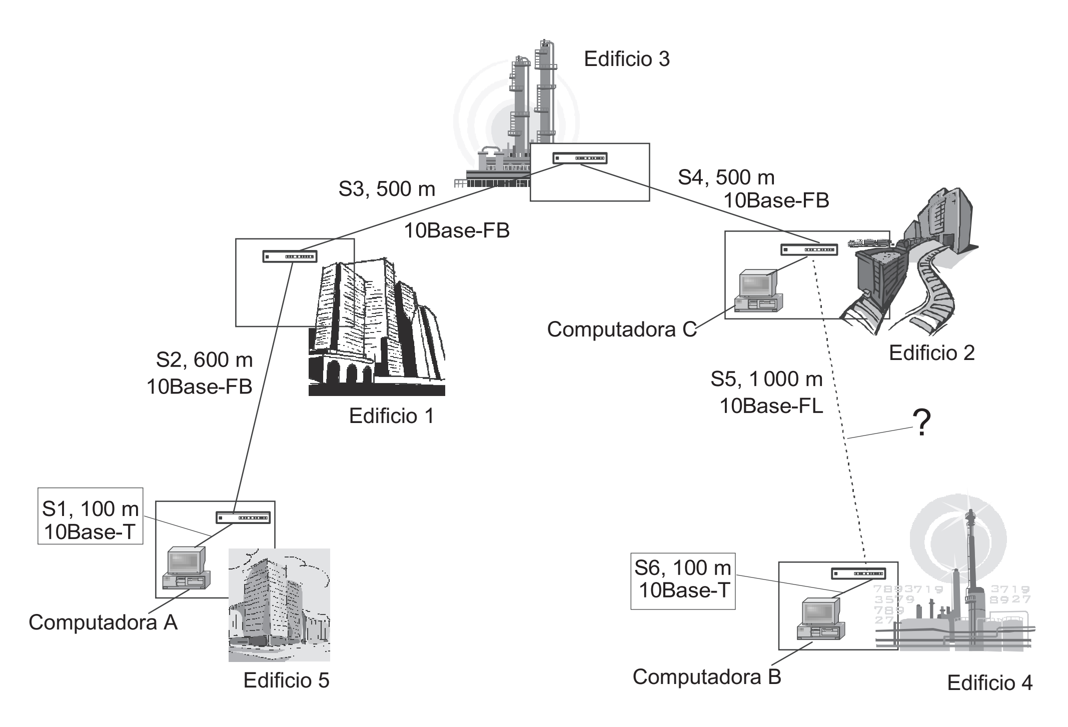


FIGURA 12.17 Red Ethernet con multisegmentos de Transmash.

que a veces se puede violar la regla de los cuatro concentradores y las limitantes en cuanto al diámetro máximo de la red, siempre que se conserve una configuración correcta. Dichas limitantes se escogieron de tal manera que garanticen una reserva significativa como márgenes de seguridad. Por ejemplo, se sabe que el PDV máximo no debe exceder de 575 bt para una detección confiable de colisiones por cualquier nodo de la red. Las técnicas que proporciona el estándar para calcular el PDV en una red 10Base-5 formada por cuatro repetidores 10Base-5 y cinco segmentos de longitud máxima (500 metros) demuestran que este intervalo es de 537 bt. Esto significa que la configuración máxima de la red 10Base-5 (cuatro concentradores y un diámetro de red de 2 500 m) tiene una reserva de 38 bt. Al mismo tiempo, el procedimiento descrito en la sección 13 del estándar 802.3 especifica que aún una reserva de 4 bt permitirá que la red trabaje de manera correcta.

Por ende, de lo anterior se infiere que el arquitecto de la red calculó una configuración posible de la planta de ingeniería de Transmash con un nuevo segmento. Como ocurrieron las cosas, aún con el edificio 4 conectado a la red, ésta hubiera tenido una reserva de 6.6 bt. Después de revisar y verificar los cálculos, se instaló un cable de fibra óptica para conectar el edificio 4 a la red de la planta y la nueva configuración de la red comenzó a trabajar. En la práctica, los cálculos resultaron ser los correctos, ya que la red completa trabajó sin ningún problema. Dicha configuración se mantuvo durante varios años hasta que los cada vez más abundantes requerimientos de las nuevas aplicaciones dieron como resultado la necesidad de dividir el medio de transmisión compartido en segmentos conmutados.

Para verificar los cálculos realizados por el arquitecto de la red de Transmash, es necesario que usted se familiarice con los detalles del procedimiento presentado en la sección 13 del estándar 802.3.

Dicho procedimiento establece que la red Ethernet trabajará correctamente siempre que se satisfagan las condiciones siguientes:

- El PDV entre las dos estaciones más distantes entre sí no debe exceder de 575 bt. Los repetidores y el medio de transmisión de los segmentos incluyen retardos adicionales en la propagación de la señal. Los datos acerca de los niveles de umbral de estos retardos se proporcionan en las tablas de la sección 13 del estándar IEEE 802.3.
- La reducción de los valores del IPG y de la variabilidad de la trayectoria (PVV) después del paso de la secuencia de tramas a través de los repetidores no debe exceder de 49 bt. Cada repetidor reduce el IPG en un valor específico, el cual es proporcionado en las tablas de la sección 13 del estándar.

Las tablas del estándar 802.3 muestran los valores máximo y mínimo de los retardos de propagación de la señal y de las reducciones de IPG posibles, pues sus valores específicos dependen del fabricante del repetidor. El arquitecto de la red Transmash utiliza datos más precisos para los cálculos que fueron proporcionados por el fabricante del equipo de la red. Dichos datos aparecen en las tablas 12.4 y 12.5.

Considere cómo evaluar el PDV mediante el uso de los datos mostrados en la tabla 12.4.

Los diseñadores del estándar 802.3 trataron de simplificar los cálculos tanto como fuera posible, por lo cual los datos contenidos en la tabla 12.5 incluyen varias etapas de la propagación de la señal. Por ejemplo, los retardos introducidos por el repetidor consisten en el retardo incluido en la entrada del transceptor, el retardo introducido por la unidad repetidora y el retardo que aparece en la salida del transceptor. No obstante, en la tabla, estos retardos están representados mediante un solo valor llamado *segmento base*.

Para no tener que adicionar los retardos introducidos por el cable dos veces, la tabla ofrece valores de retardos dobles por cada tipo de cable.

TABLA 12.4 Datos para el cálculo del PDV

Tipo de segmento	Base del segmento izquierdo (bt)	Base del segmento intermedio (bt)	Base del segmento derecho (bt)	Retardo medio por metro (bt)	Longitud máxima del segmento (m)
10Base-5	11.8	46.5	169.5	0.0866	500
10Base-2	11.8	46.5	169.5	0.1026	185
10Base-T	15.3	42.0	165.0	0.113	100
10Base-FB	__	24.0	__	01	2 000
10Base-FL	12.3	33.5	156.5	0.1	2 000
FOIRL	7.8	29.0	152.0	0.1	1 000
AUI (>2 m)	0	0	0	0.1026	2 048

En la tabla también se incluyen definiciones como *segmento izquierdo*, *segmento derecho* y *segmento intermedio.* Cabe aclarar estos términos en el caso de la planta de ingeniería de Transmash (figura 12.17). El objetivo es calcular el PDV para el peor caso, por lo que se seleccionarán los nodos A y B, los cuales están separados mediante cinco repetidores y hay 2 800 metros de red entre ellos.

De acuerdo con la terminología del estándar 802.3, en el segmento izquierdo comienza la trayectoria de la señal de la salida del transmisor en el nodo terminal. El término izquierdo no está relacionado de ninguna manera con la ubicación geográfica de los segmentos (o con su ubicación en el diagrama): simplemente es un nombre convencional del segmento a partir del cual comienzan los cálculos. Seleccione el segmento S1, al cual está conectado el nodo A, como el segmento izquierdo de la red.

Después de hacer lo anterior, la señal pasa a través de los segmentos intermedios S2-S5 y llega al receptor (nodo B), conectado al segmento S6. Éste es el punto en el que, en el peor de los casos, se presenta una colisión, lo cual se considera en la tabla. El segmento terminal, donde ocurre la colisión, se conoce como segmento derecho.

Cada segmento introduce un retardo constante conocido como **base**, el cual depende solamente del tipo de segmento y de su posición a lo largo de la trayectoria de la señal (izquierdo, intermedio o derecho). La base del segmento derecho, donde surge la colisión, excede de manera significativa las bases de los segmentos izquierdo e intermedio.

Además de lo anterior, cada segmento introduce un retardo en la propagación de la señal, el cual depende de la longitud del segmento y se calcula al multiplicar el tiempo de propagación de la señal por un metro de cable (en intervalos de bit) por la longitud del cable (en metros).

El cálculo incluye la evaluación de los retardos introducidos por cada sección de cable (la longitud que se proporciona en la tabla del retardo de la señal por metro de cable se multiplica por la longitud del segmento). Después, estos retardos se suman a las bases de los segmentos izquierdo, intermedio y derecho.

Como los segmentos izquierdo y derecho tienen diferentes valores de retardo base, los cálculos deben realizarse dos veces si hay diversos tipos de segmentos en los extremos

distantes de la red. Primero, es necesario llevar a cabo una evaluación cuando se considera un tipo de segmento como el izquierdo y repetir el cálculo tomando otro tipo de segmento como el segmento izquierdo. El PDV máximo debe seleccionarse como resultado final, en cuyo caso, los segmentos terminales son del mismo tipo, es decir, 10Base-T; por lo tanto, no es necesario llevar a cabo un doble cálculo.

Ahora ya se puede calcular el PDV:

- Segmento izquierdo S1:

  15.3 (base) + $(100 \times 0.113) = 26.6$
- Segmento intermedio S2:

  $24 + (600 \times 0.1) = 84.0$
- Segmento intermedio S3:

  $24 + (500 \times 0.1) = 74.0$
- Segmento intermedio S4:

  $24 + (500 \times 0.1) = 74.0$
- Segmento intermedio S5:

  $33.5 + (1\,000 \times 0.1) = 133.5$
- Segmento derecho S6:

  $165 + (100 \times 0.113) = 176.3$

La suma de estos componentes da un PDV de 568.4.

Como el PDV es más pequeño que el valor máximo 575 permitido por 6.6 bt, la configuración de la red es correcta, aun cuando su longitud total exceda de 2 500 m y tenga más de cuatro repetidores.

No obstante, la verificación del PDV no es suficiente para llegar a una conclusión positiva, sino también es necesario evaluar el PVV.

Los puntos iniciales para el cálculo del PVV se proporcionan en la tabla 12.5.

De acuerdo con la información siguiente, calcule el PVV del ejemplo:

- Segmento izquierdo 1 10Base-T: 10.5 bt
- Segmento intermedio 2 10Base-FL: 8
- Segmento intermedio 3 10Base-FB: 2
- Segmento intermedio 4 10Base-FB: 2
- Segmento intermedio 5 10Base-FB: 2

TABLA 12.5 Reducción del IPG mediante repetidores

Tipo de segmento	Segmento de transmisión (bt)	Segmento intermedio (bt)
10Base-5 o 10Base-2	16	11
10Base-FB	—	2
10Base-FL	10.5	8
10Base-T	10.5	8

La suma de estos valores da un PVV de 24.5, el cual es menor que el umbral de 49 bt. Como resultado, se puede concluir que la red del ejemplo corresponde a los estándares Ethernet para todos los parámetros: tanto la longitud del segmento como el número de repetidores.

RESUMEN

- Las LAN compartidas son las implementaciones de LAN más sencillas y baratas. La desventaja principal de las LAN son su bajo nivel de escalabilidad, pues al aumentar el número de nodos, la parte del ancho de banda total asignada a cada nodo se reduce en la misma proporción.
- El comité 802 del IEEE desarrolla estándares que contienen recomendaciones para el diseño de las capas inferiores de las LAN: física y de enlace de datos. Las características físicas de las LAN se reflejan en la división de la capa de enlace de datos en dos subcapas: LLC y MAC.
- La subcapa MAC es responsable del acceso al medio de transmisión compartido y los utiliza para enviar tramas. Los estándares IEEE 802 emplean varios métodos de acceso divididos en dos categorías: aleatorios y determinísticos. Los métodos de acceso aleatorios garantizan un retardo de acceso al medio de transmisión mínimo en condiciones de baja carga de tráfico. A pesar de ello, a medida que el empleo del medio de transmisión se aproxima al 100%, el uso de métodos de acceso aleatorios da como resultado grandes valores de retardo. Los métodos determinísticos son capaces de trabajar con mayores cargas de tráfico en la red.
- Los estándares del grupo de trabajo 802.1 son comunes a todas las tecnologías y definen los tipos de LAN, sus propiedades, procedimientos de interconectividad y la lógica de operación de los puentes y ruteadores.
- El protocolo LLC garantiza la calidad de servicios de transporte requerida para los protocolos de las capas superiores. Dicho protocolo podrá transmitir tramas si utiliza transmisión de datagramas o procedimientos para establecer conexiones y recuperar tramas.
- En la actualidad, Ethernet es la tecnología de LAN más común y extendida por el mundo. En un sentido amplio, Ethernet es una familia de tecnologías que incluye el estándar propietario Ethernet DIX y estándares abiertos, como el Ethernet IEEE 802.3 a 10 Mbps, Fast Ethernet, Gigabit Ethernet y 10 G Ethernet. Todos estos tipos, excepto 10G Ethernet, utilizan el mismo método de acceso —CSMA/CD— el cual, en muchos sentidos, define las características de la tecnología.
- Una colisión es un evento importante típico de Ethernet que sucede cuando dos estaciones de trabajo intentan de manera simultánea transmitir tramas de datos a través del medio de transmisión común. La presencia de colisiones es una propiedad natural de Ethernet y representa una consecuencia del método de acceso aleatorio adoptado. La posibilidad de detectar colisiones de manera confiable depende de la elección correcta de los parámetros de la red, particularmente al observar la relación que existe entre la longitud de la trama y el diámetro máximo de la red.
- El empleo máximo del segmento Ethernet a 10 Mbps tramas por segundo se logra cuando se transmiten tramas de longitud mínima: es de 14 880 fps. Al mismo tiempo, el ancho de banda efectivo de la red es de solamente 5.48 Mbps, un valor un poco mayor que la mitad del ancho de banda nominal: 10 Mbps.

- El ancho de banda máximo alcanzable en Ethernet es de 9.75 Mbps, que corresponde al uso de tramas de longitud máxima de 1 518 bytes transmitidas a 513 fps.
- Ethernet soporta cuatro tipos de tramas que tienen el mismo formato de direcciones de nodos. Existen reglas formales de acuerdo con las cuales los adaptadores de red reconocen automáticamente el tipo de trama.
- En función del tipo de medio de transmisión físico, el estándar 802.3 del IEEE define distintas especificaciones: 10Base-5, 10Base-2, 10Base-T, FOIRL, 10Base-FL o 10Base-FB. Para cada especificación se definen las características siguientes: tipo de cable, longitud máxima de segmentos de cable continuos y las reglas para usar repetidores con el fin de incrementar el diámetro de la red, por ejemplo: la regla 5-4-3 para las redes de cable coaxial y la regla de los cuatro concentradores para las redes de par trenzado y fibra óptica.

PREGUNTAS DE REPASO

1. Explique la diferencia entre extensibilidad y escalabilidad de la red, con base en el ejemplo de Ethernet.
2. Compare los métodos aleatorios y determinísticos de acceso al medio de transmisión compartido.
3. ¿Por qué los protocolos de la capa de enlace de datos de las tecnologías WAN no se dividen en las subcapas MAC y LLC?
4. ¿Qué funciones realiza la capa LLC?
5. ¿Qué es una colisión?
6. ¿Cuáles son las funciones del preámbulo y del delimitador de trama en el estándar Ethernet?
7. ¿Qué herramientas de red llevan a cabo el control del parloteo?
8. ¿Por qué se introdujo en Ethernet el espacio entre paquetes?
9. ¿Cuáles son los valores de las características del estándar 10Base-5 que se mencionan a continuación?
   - Ancho de banda nominal (bps).
   - Ancho de banda efectivo (bps).
   - Utilización (fps).
   - Velocidad de transmisión entre paquetes (bps).
   - Espacio entre bits (seg).
10. ¿Por qué se fijó el tamaño mínimo de trama en el estándar 10Base-5 a 64 bytes?
11. ¿Por qué los estándares 10Base-T y 10Base-FL/FB han sacado de competencia a los estándares Ethernet por cable coaxial?
12. Explique el significado de cada uno de los campos de la trama Ethernet.
13. Existen cuatro estándares que rigen el formato de trama de Ethernet. De la lista que se proporciona aquí, seleccione los nombres de dichos estándares, sin olvidar que algunos de ellos tienen varios nombres:
    a) 802.2 de Novell
    b) Ethernet II
    c) 802.3/802.2
    d) 802.3 de Novell
    e) 802.3 a secas

f) DIX de Ethernet
g) 802.3/LLC
h) SNAP de Ethernet

14. ¿Qué puede suceder en una red en la que se transmitan tramas de Ethernet con formatos diferentes?
15. ¿De qué manera influye el valor del tamaño de paquete en la operación de la red?, ¿qué problemas se relacionan con el uso de tramas muy largas?, ¿por qué son ineficaces las tramas cortas?
16. ¿De qué manera influye el coeficiente de utilización en el desempeño de una red Ethernet?
17. ¿De qué manera influye la velocidad de transmisión de datos de una red Ethernet de medio de transmisión compartido en el diámetro máximo de la red?
18. ¿Qué consideraciones influyen en la selección de la longitud máxima de segmento físico en los estándares de Ethernet?
19. ¿Qué permitió que la longitud máxima del segmento se incrementara durante el cambio del estándar FOIRL al 10Base-FL?
20. ¿Cuál fue la razón que dio lugar a la limitante conocida como regla de los cuatro concentradores?
21. ¿Por qué el modo full-duplex de Ethernet no es soportado por los concentradores?

PROBLEMAS

1. ¿Representan dominios de colisión los fragmentos de red que se muestran en la figura 12.18?

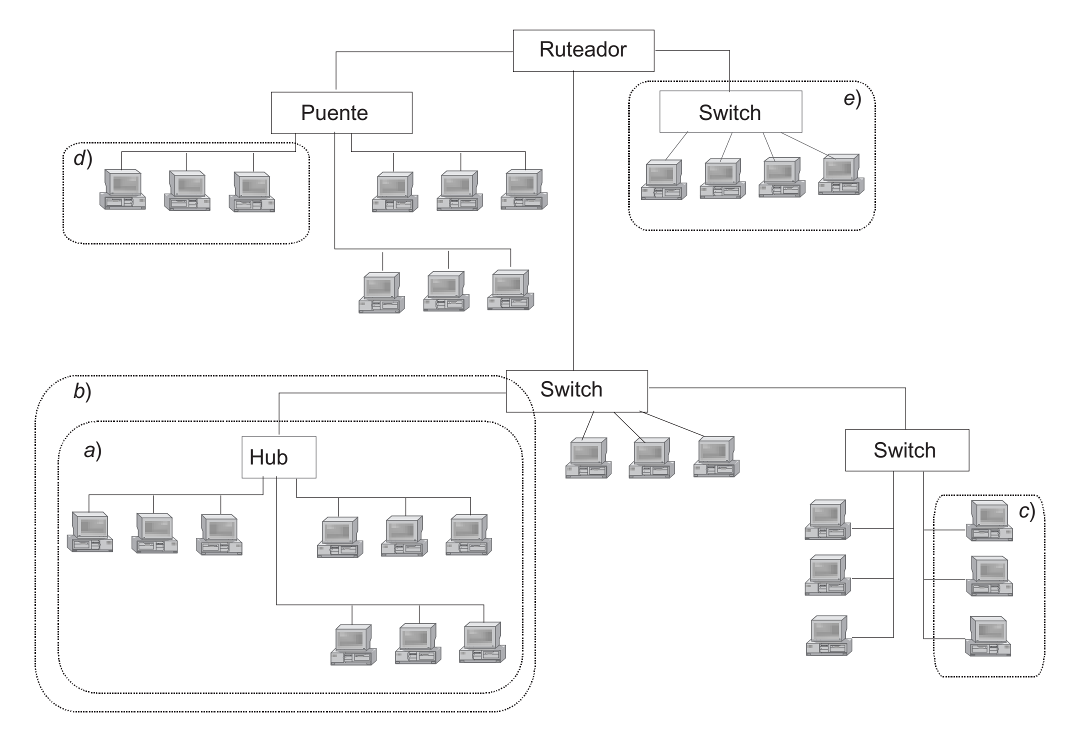


FIGURA 12.18 Posibles dominios de colisión.

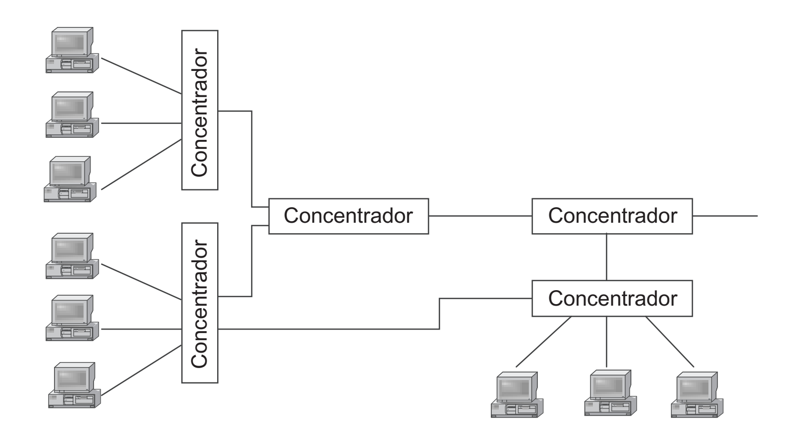


FIGURA 12.19 Loops en una red Ethernet construida con base en concentradores.

2. ¿Cuánto tiempo puede esperar una estación de trabajo antes de que su trama sea descartada por el adaptador de red?

3. ¿Qué pasará en una red instalada con base en concentradores si hay circuitos cerrados (loops) en ésta, como los que se muestran en la figura 12.19?

a) La red trabajará normalmente.

b) Las tramas no llegarán al nodo de destino.

c) Se presentarán colisiones cuando se intente transmitir una trama.

d) Las tramas quedarán confinadas en un loop.

4. Evalúe la disminución del desempeño de una red Ethernet cuando transmite un archivo de 240 000 bytes, si el nivel de pérdida o de tramas dañadas se incrementa de 0 a 3%. La operación de la red se muestra en la figura 12.20.

El archivo se transmite por medio de los protocolos siguientes: Ethernet, IPX (capa de red) y NCP (capa de aplicación del servicio de archivos). Los tamaños de los encabezados de los protocolos son los siguientes:

- Ethernet: 26 bytes (con un preámbulo y un campo FCS)
- IPX: 30 bytes
- NCP: 20 bytes

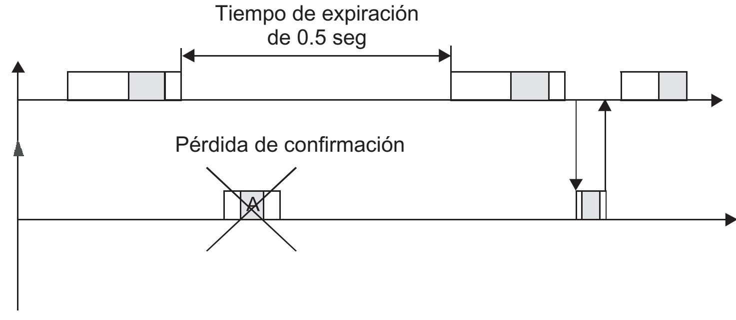
El archivo se transmite en segmentos de 1 000 bytes. Solamente el NCP que trabaja de acuerdo con el *método de la fuente desocupada* puede recuperar las tramas dañadas o perdidas. El tiempo de expiración de reconocimientos positivos está fijo en 500 mseg. (Éste no es el único modo de operación del NCP: también podrá trabajar si utiliza el algoritmo de ventana deslizante. A pesar de ello, en este caso no se usa dicho modo.) El tamaño del reconocimiento es de 10 bytes. El tiempo de procesamiento en un solo paquete en el lado del cliente es de 650 μseg y del lado del servidor es de 50 μseg.

SUGERENCIA *El problema se puede dividir en dos partes. Primero, es necesario determinar la velocidad real de la transmisión del archivo en condiciones de operación ideales de la red, cuando el porcentaje de tramas perdidas o dañadas de Ethernet sea cero. La segunda parte del problema requiere determinar la velocidad de transmisión de archivos cuando las tramas comiencen a perderse o a dañarse.*

a) Modo de operación normal

Paquetes del servidor
Periodo de transmisión
Tiempo de procesamiento en el servidor
E IPX NCP Data A
Confirmaciones del cliente
Tiempo de procesamiento en el cliente
A

b) Pérdidas de paquetes



E Encabezado de la trama de Ethernet
PX Encabezado del paquete IPX
NCP Encabezado del paquete NCP
A Confirmación

FIGURA 12.20 Operación de una red Ethernet durante la transmisión de archivos.

La transmisión de archivos necesitará 240 paquetes en total. El tamaño de una trama Ethernet que transporta 1 000 bytes del archivo que se transmite será de 1 000 + 20 + 30 + 26 = 1 076 bytes u 8 608 bits.

El tamaño de la trama Ethernet que transporta el reconocimiento es de 86 bytes (contando el preámbulo) o de 688 bits.

En estas condiciones, el tiempo de un solo ciclo de transmisión de la parte siguiente del archivo en una red ideal será de 860.8 + 68.8 + 650 + 50 = 1 629.6 mseg.

El tiempo requerido para transmitir un archivo de 240 000 bytes será de 240 × 1 629.6 = 0.391 seg y la velocidad de información será de 240 000/0.391 = 613 810 bps.

Ahora sólo queda encontrar la velocidad de información cuando las tramas comiencen a perderse o a dañarse.

13

ETHERNET DE ALTA VELOCIDAD

DESCRIPCIÓN DEL CAPÍTULO

13.1 INTRODUCCIÓN

El Ethernet clásico de 10 Mbps pudo satisfacer a la mayoría de los usuarios durante unos 15 años, pero a principios de la década de 1990 comenzó a ser evidente la insuficiencia de su ancho de banda. La tasa de intercambio de 10 Mbps fue significativamente más pequeña que las tasas del bus interno de las computadoras, las cuales por esa época habían excedido el umbral de los 1 000 Mbps (el bus PCI aseguraba la transmisión de datos a 133 MB/s). Esto resultaba en un funcionamiento más lento de la red no sólo para los servidores, sino también para las estaciones de trabajo, que comenzaban a utilizar el bus PCI.

La necesidad de contar con una nueva tecnología para Ethernet fue evidente. Esta nueva tecnología tenía que ser tan eficaz como la tecnología anterior en términos de su relación calidad/precio y para asegurar un rendimiento a 100 Mbps. En el curso de la investigación y desarrollo, los especialistas se dividieron en dos grupos y crearon en 1995 dos nuevas tecnologías: Fast Ethernet y 100VG-AnyLAN. Sin embargo, a la larga, únicamente sobrevivió Fast Ethernet (que conservó más propiedades del Ethernet clásico, incluida CSMA/CD).

El éxito de Fast Ethernet aumentó más el interés en el Ethernet de alta velocidad. La variante siguiente, Gigabit Ethernet, se estandarizó tres años después y también se distingue por el alto nivel de características conservadas del Ethernet de 10 Mbps; asimismo, ha mantenido la posibilidad de funcionar en un medio compartido utilizando CSMA/CD.

No obstante, la versión más reciente de Ethernet, 10G Ethernet, difiere de manera considerable de su antecesor. En particular, funciona sólo en el modo full-dúplex, lo cual significa que ya no soporta un medio compartido.

Por lo tanto, en este capítulo se considerarán únicamente Fast Ethernet y Gigabit Ethernet. 10G Ethernet se estudiará en el capítulo 15, con otras tecnologías que funcionan en el modo full-dúplex que permite la construcción de LAN conmutadas.

13.2 FAST ETHERNET

PALABRAS CLAVE: *Fast Ethernet Alliance*, 100Base-TX, 100Base-FX, prioridad por la demanda, subcapa de reconciliación de la interfaz independiente del medio (MII y Media Independent Interface), dispositivo de capa física (PHY y Physical Layer Device), símbolo nulo, autonegociación, 100Base-TX full-dúplex, ráfaga de pulso rápido de enlace (FLP y Fast Link Pulse), puerto de interfaz dependiente del medio (MDI y Medium Dependent Interface), puerto MDI-X, limitaciones en la longitud máxima, repetidores clase I y II, Fast Ethernet, regla de uno o dos concentradores (hubs) y 100VG-AnyLAN.

13.2.1 Perspectiva histórica

En 1992, un grupo de fabricantes de equipo para redes, incluidos líderes de Ethernet como SynOptics y 3Com, crearon la *Fast Ethernet Alliance* sin fines de lucro. El objetivo principal de esta alianza fue diseñar el estándar para la nueva tecnología, la cual tenía que asegurar un considerable desarrollo en rendimiento, pero al mismo tiempo conservar tantas características específicas de Ethernet como fuera posible.

Al mismo tiempo, el comité IEEE 802 había formado un grupo de investigación para estudiar el potencial tecnológico de las nuevas tecnologías de alta velocidad. Desde finales de 1992 hasta finales de 1993, el grupo de la IEEE estudió varias soluciones de 100 Mbits sugeridas por diversos fabricantes. Además de los propósitos de la Fast Ethernet Alliance,

el grupo también consideró la tecnología de alta velocidad sugerida por Hewlett-Packard y AT&T.

El problema de mantener CSMA/CD estuvo en el centro de la discusión. La sugerencia de la Fast Ethernet Alliance conservaba este método, proporcionando compatibilidad y coordinación entre las tecnologías de 10 Mbps y de 100 Mbps. La coalición HP/AT&T, que era apoyada por un número de fabricantes de equipos de redes significativamente más pequeño que el de la Fast Ethernet Alliance, sugirió un método de acceso diferente y más novedoso, que llegó a ser conocido como **prioridad por la demanda**. Este método cambió de manera significativa el patrón de comportamiento del nodo de la red y, por lo tanto, no podía ser mezclado con Ethernet y el IEEE 802.3. Un nuevo grupo de trabajo de la IEEE (IEEE 802.12) se organizó para estandarizar la prioridad por la demanda.

En el otoño de 1995, ambas tecnologías se convirtieron en estándares de la IEEE. El comité IEEE 802.3 adoptó Fast Ethernet como el estándar 802.3u. El IEEE 802.3u no es un estándar autónomo, pero sí un suplemento al estándar 802.3 existente en la forma de los capítulos 21-30. El comité 802.12 adoptó 100VG-AnyLAN, el cual utiliza el nuevo método de acceso por prioridad por la demanda y soporta tramas de dos formatos: Ethernet y Token Ring.

13.2.2 Capa física del Fast Ethernet

Todas las diferencias entre las tecnologías de Fast Ethernet y del Ethernet clásico están concentradas en la capa física (figura 13.1). En el Fast Ethernet, las capas MAC y LLC permanecen igual y están descritas en los mismos capítulos de los estándares 802.3 y 802.2; por lo tanto, para Fast Ethernet, se considerarán aquí solamente unas cuantas versiones de su capa física.

La estructura más compleja de la capa física del Fast Ethernet se debe al uso de tres variantes de sistemas de cableado:

- Cable multimodal de fibra óptica, de dos fibras.
- Par trenzado categoría 5, dos pares.
- Par trenzado categoría 3, cuatro pares.

El cable coaxial que dio al mundo su primera red Ethernet no fue incluido en la lista de medios de transmisión permitidos para Fast Ethernet. Esta tendencia es común para la mayoría de las nuevas tecnologías, pues el par trenzado categoría 5 permite la transmisión de datos a la misma velocidad que el cable coaxial. Al mismo tiempo, la red se hace más económica y más conveniente para soporte y mantenimiento. Para distancias más grandes, la fibra óptica proporciona un ancho de banda bastante más amplio que el cable coaxial y el costo de la red sólo es un poco más alto, en especial si se tiene en cuenta el alto costo del rastreo de fallas de funcionamiento y de la detección de fallas en un sistema de cableado coaxial extenso.

Debido a que el uso del cable coaxial fue desechado, las redes Fast Ethernet sobre un medio compartido siempre tienen una estructura de árbol jerárquico basada en concentradores de manera similar a la de las redes 10Base-T/10Base-F. La diferencia principal en las configuraciones Fast Ethernet es la reducción del diámetro de la red hasta alrededor de 200 m. Esto se explica por la reducción en 10 veces el tiempo requerido para transmitir una trama de longitud mínima debido al incremento en 10 veces la velocidad de transmisión de datos en comparación con el Ethernet clásico.

Sin embargo, esto no presenta un obstáculo serio para construir redes extensas basadas en Fast Ethernet. A mediados de la década de 1990 se caracterizaron no sólo por el amplio

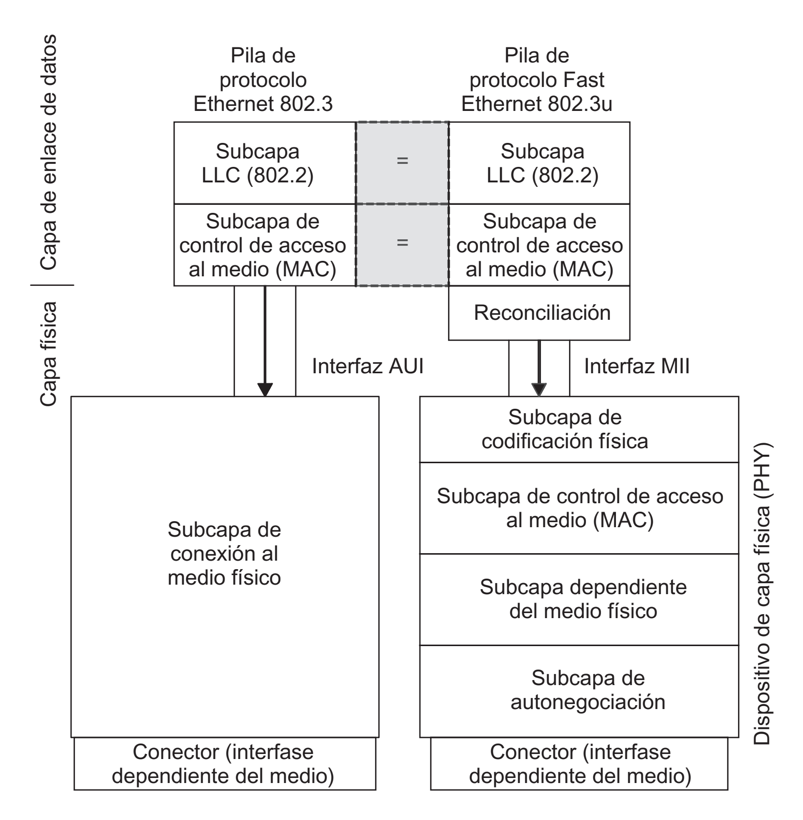


FIGURA 13.1 Diferencias entre Fast Ethernet y Ethernet clásico.

uso de tecnologías económicas de alta velocidad, sino también por el rápido desarrollo de las LAN *conmutadas*. Cuando se utilizan switches, Fast Ethernet puede funcionar en el modo full-dúplex, el cual no impone limitaciones acerca de la longitud total de la red. Cuando se usa el modo full-dúplex, las únicas limitaciones que se mantienen son con respecto a la longitud de los segmentos físicos que conectan dispositivos cercanos (como un adaptador-switch o un switch-switch).

En esta sección la atención se centrará en la variante clásica, half-dúplex del funcionamiento de Fast Ethernet, que corresponde por entero a la definición del método de acceso en el estándar 802.3. Las características específicas del modo full-dúplex del funcionamiento de Fast Ethernet se estudiarán en el capítulo 15.

En comparación con las implementaciones físicas del Ethernet clásico (existen seis), en el Fast Ethernet las diferencias entre las variantes de capa física son más significativas. Esto se debe a que tanto el número de conductores como el método de codificación cambian de una implementación a otra. Además, las implementaciones físicas del Fast Ethernet fueron creadas de manera simultánea, en vez de evolucionar, como ocurrió con el Ethernet clásico. Por lo tanto, fue posible definir con detalle subcapas de una capa física que no cambian con versiones y subcapas específicas para cada variante de un medio físico.

El estándar oficial 802.3 define tres especificaciones para la capa física del Fast Ethernet (figura 13.2):

- **100Base-TX** para cable de dos pares basado en un par trenzado sin blindaje (UTP, Unshielded Twisted Pair) de categoría 5 o un par trenzado blindado (STP, Shielded Twisted Pair) de tipo 1.
- **100Base-T4** para cable de cuatro pares basado en UTP de categoría 3, 4 o 5.

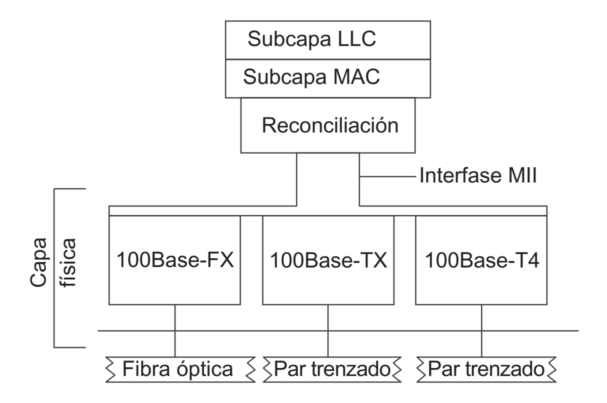


FIGURA 13.2 Estructura de la capa física de Fast Ethernet.

- **100Base-FX** para cable de fibra óptica multimodal utilizando dos fibras.

Los enunciados siguientes son verdaderos para las tres especificaciones:

- Los formatos de trama del Fast Ethernet no difieren de los formatos de trama utilizados en el Ethernet de 10Mbps.
- La banda entre paquetes (IPG, por sus siglas en inglés para InterPacket Gap) es de 0.96 µseg y el intervalo de bits (bt) es de 10 nseg. Todos los parámetros temporales del algoritmo de acceso (tiempo de ranura, tiempo requerido para transmitir la trama de longitud mínima, etc.) se miden en intervalos de bits y permanecen iguales, de modo que no se hicieron cambios en las secciones del estándar relacionadas con la capa MAC.
- La transmisión del símbolo Idle (nulo o libre) del código redundante apropiado utilizando el medio indica su disponibilidad (en contraste con los estándares del Ethernet de 10 Mbps, donde la carencia de las señales indica que el medio está libre).

La capa física incluye tres elementos:

- **Interfaz independiente del medio (MII,** por sus siglas en inglés para **Media Independent Interface).**
- **Subcapa de reconciliación**, necesaria para habilitar la capa MAC, destinada para funcionar con la AUI, para comunicarse con la capa física utilizando la MII.
- **Dispositivo de capa física** (**PHY**, por sus siglas para **PHYsical layer device**), que, a su vez, comprende varias subcapas (véase la figura 13.1):
  - **Subcapa de codificación física** (**PCS,** por sus iniciales, correspondientes a **Physical Coding Sublayer**), la cual transforma los bytes que llegan desde la capa MAC en símbolos 4B/5B o 8B/6T (ambos códigos se utilizan en Fast Ethernet).
  - Las subcapas de **conexión del medio físico** (**PMA,** por **Physical Medium Attachment**) **y dependiente del medio físico** (**PMD**, por **Physical Medium Dependent**), que aseguran la formación de señales eléctricas u ópticas tales como NZRI o MLT-3.
  - **Subcapa de autonegociación**, la cual permite a dos puertos en interacción seleccionar de modo automático el modo de funcionamiento más eficaz, por ejemplo: half-dúplex o full-dúplex. Esta subcapa es opcional.

MII soporta un método independiente del medio de intercambio de datos entre las subcapas MAC y PHY. Por su objetivo, esta interfaz es semejante a la AUI del Ethernet clásico, excepto la AUI que residía entre la subcapa de señalización de capa física (PLS, por Physical

Layer Signaling) (con un cable diferente se utilizaba el mismo método de codificación física, el código Manchester) y la subcapa PMA. Por otro lado, MII reside entre la subcapa de reconciliación de la capa MAC y la PCS, que soporta dos métodos de codificación, como se mencionó con anterioridad. PCS, PMA y PMD forman la subcapa PHY, de la cual existen tres versiones en Fast Ethernet: FX, TX y T4 (figura 13.2).

13.2.3 Especificaciones 100Base-FX/TX/T4

Las especificaciones 100Base-FX, 100Base-TX y 100Base-T4 tienen mucho en común; por consiguiente, las propiedades comunes a estas especificaciones se considerarán con nombres generalizados, por ejemplo, 100Base-FX/TX o 100Base-TX/T4.

La especificación *100Base-FX* (fibra óptica multimodal, dos fibras) define la operación del protocolo de Fast Ethernet en los modos half-dúplex y full-dúplex.

En contraste con Ethernet de 10 Mbps, que utiliza el código Manchester para la representación de datos cuando estos se transmiten por el cable, Fast Ethernet define otro método de codificación: 4B/5B. Los detalles de la codificación 4B/5B se estudiaron en el capítulo 9. Antes que fuera diseñado Fast Ethernet, este método había demostrado su eficacia en redes FDDI y, por lo tanto, fue introducido sin cambios en 100Base-FX/TX. En este método, los cuatro bits de los datos de la subcapa MAC (conocidos como *símbolos*) están representados por cinco bits. El bit redundante permite utilizar códigos potenciales cuando se representa cada uno de los cinco bits en la forma de pulsos eléctricos u ópticos.

La existencia de violaciones de código debidas a la redundancia de 4B/5B y 8B/6T permite descartar los símbolos erróneos y mejorar la estabilidad de las redes 100Base-FX/TX. De este modo, la indicación de disponibilidad del medio en Fast Ethernet es la transmisión repetida del *símbolo "Idle" o libre (11111)*, que constituye una violación de código cuando se codifican los datos del usuario. Un método de esta clase permite al receptor estar siempre sincronizado con el transmisor.

Para separar la trama de Ethernet de los símbolos libres se utiliza la combinación de limitador de inicio, el cual consta de dos símbolos: *J(11000)* y *K(10001)* del código 4B/5B. Cuando se completa la transmisión de la trama, el símbolo *T* se inserta antes del primer símbolo libre (figura 13.3).

Después de convertir segmentos de cuatro bits de los códigos MAC en segmentos de la capa física de cinco bits, deben estar representados como señales ópticas o eléctricas transmitidas en el cable que se conecta a los nodos de la red. 100Base-FX y 100Base-TX utilizan diversos métodos de codificación de línea: NRZI y MLT-3, respectivamente.

La especificación *100Base-TX* usa un cable UTP categoría 5 o STP tipo 1 (dos pares) como un medio de transmisión. Sus diferencias principales respecto a la especificación 100Base-FX son el uso del método MLT-3 para transmitir señales (segmentos de cinco bits de código 4B/5B) utilizando un par trenzado, además de la presencia de la función de autonegociación para seleccionar el modo de operación del puerto.

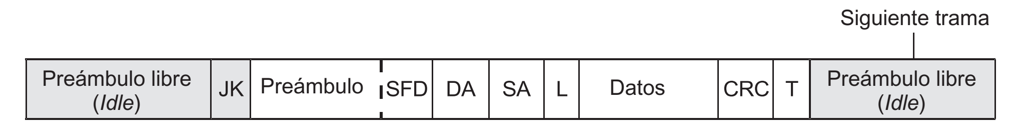


FIGURA 13.3 Flujo continuo de datos en 100Base-FX/TX.

El método de **autonegociación** permite que dos dispositivos conectados de manera física soporten diferentes estándares de capa física en términos de velocidad de bits y número de pares trenzados para elegir el modo de operación más eficaz. Por lo regular, el procedimiento de autonegociación tiene lugar cuando se conecta un adaptador de redes capaces para funcionar a 10 y 100 Mbps al switch o enrutador.

Los dispositivos 100Base-TX/T4 basados en un par trenzado soportan cinco modos de operación:

- 10Base-T.
- 10Base-T full-dúplex.
- 100Base-TX.
- 100Base-T4.
- 100Base-TX full-dúplex.

10Base-T tiene la prioridad más baja en el curso de la negociación, mientras que el modo 100Base-TX full-dúplex tiene la prioridad más alta.

El proceso de negociación tiene lugar cuando el dispositivo se activa; también puede ser iniciado en cualquier momento mediante la unidad de control del dispositivo.

El dispositivo que ha iniciado el proceso de autonegociación envía a su asociado una secuencia de pulsos especiales, llamada **ráfaga de pulsos de enlace rápidos (FLP,** por sus siglas para **Fast Link Pulse)**, que contienen una palabra de ocho bits que codifica el modo propuesto de interacción, a partir del modo de prioridad más alta soportado por el nodo actual.

Si el nodo asociado soporta la función de autonegociación y el modo propuesto, responderá con otra ráfaga FLP, lo que será una confirmación del modo propuesto. El proceso de negociación se completa en este punto. Si el nodo asociado solamente puede soportar el modo de prioridad más baja, especifica este modo en su respuesta, el cual se elige como el modo de operación. De esta manera, siempre se elige el modo de prioridad más alta comúnmente soportado.

La especificación *100Base-T4* (UTP de categoría 3, cuatro pares) apareció mucho después que otras especificaciones de capa física para Fast Ethernet. El objetivo principal de los diseñadores de las primeras tecnologías, 100Base-TX/FX, fue especificar una capa física tan cercana como fuera posible a 10Base-T y 10Base-F que funcionara sobre dos enlaces de transmisión de datos: dos pares trenzados o dos fibras ópticas. Para implementar el funcionamiento sobre dos pares trenzados, fue necesario cambiar al cable de categoría 5, el cual se caracteriza por su calidad superior.

Al mismo tiempo, los diseñadores de la tecnología competidora 100VG-AnyLAN inicialmente admitieron el funcionamiento utilizando un par trenzado de categoría 3. La principal ventaja de esta solución residía no tanto en su precio económico, sino en el cableado requerido que se encontraba instalado en la mayoría de los edificios. Por ende, después de que 100Base-TX y 100Base-FX fueron liberados, los diseñadores de Fast Ethernet también implementaron su versión de la capa física para el par trenzado de categoría 3.

En lugar de la codificación 4B/5B, este método utiliza codificación 8B/6T, caracterizada por un espectro de señales más estrecho. A 33 Mbps, este método se ajusta dentro de la banda de 16 MHz del par trenzado categoría 3 (cuando se usa una codificación 4B/5B, el espectro de señales no se ajusta dentro de esta banda). Cada segmento de ocho bits de información de la capa MAC está codificada por seis símbolos ternarios (es decir, mediante dígitos con tres estados). La transmisión de cada dígito ternario dura 40 nseg. El grupo de seis dígitos ternarios se pasa luego a uno de los tres pares trenzados de transmisión, de manera independiente y secuencial.

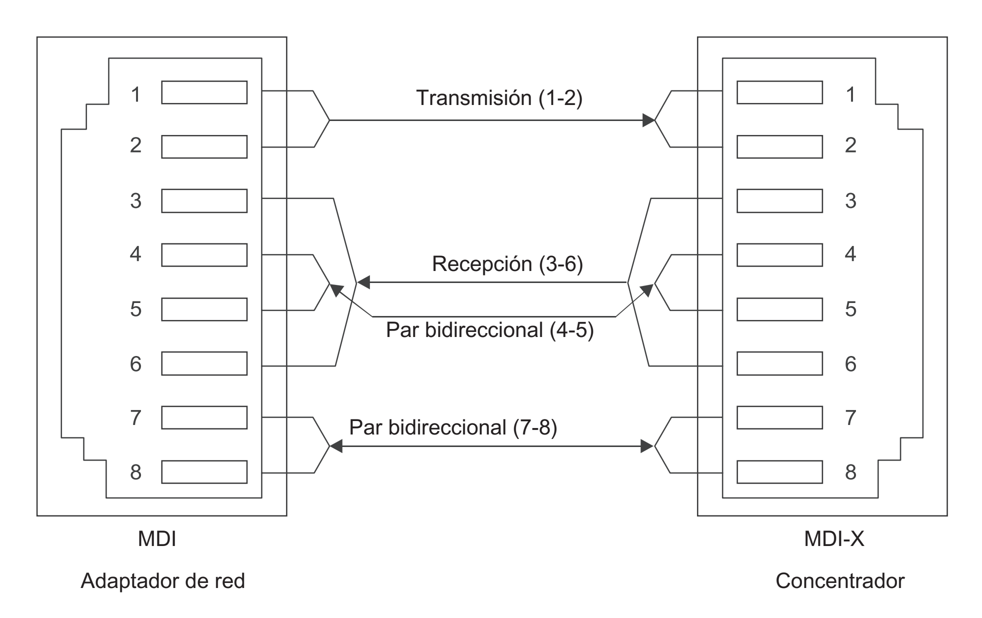


FIGURA 13.4 Conexión de nodos en 100Base-T4.

El cuarto par se utiliza siempre con el fin de sensibilizar al portador para detectar colisiones. La velocidad y transmisión sobre cada uno de los tres pares de transmisión es de 33.3 Mbps, de modo que la velocidad total del protocolo 100Base-T4 es de 100 Mbps. Al mismo tiempo, debido al método de codificación adoptado, la velocidad del cambio de señal en cada par es de solamente 25 Mbaudios, de manera que puede ser utilizado el par trenzado de categoría 3.

La figura 13.4 muestra la conexión de un *puerto* **MDI** (Medium Dependent Interface, es decir, interfaz dependiente del medio) de un adaptador de red 100Base-T4 hacia el **puerto MDI-X** del concentrador. (El sufijo X indica que en este puerto, los contactos que conectan el receptor y el transmisor son intercambiados para enrutar las señales de transmisión de una pieza de equipo a las señales que se reciben de otra pieza de equipo y viceversa, lo que proporciona una manera más fácil de unir pares en el cable sin cruzarlos.) El par 1-2 se requiere para transmitir datos desde el puerto MDI hasta el puerto MDI-X, el par 3-6 es para la recepción de datos por el puerto MDI desde el puerto MDI-X y los pares 4-5 y 7-8 son bidireccionales y se utilizan tanto para la transmisión como para la recepción como sea necesario.

13.2.4 Reglas para construir segmentos de Fast Ethernet utilizando repetidores

Fast Ethernet, al igual que todas las variantes de Ethernet, está destinado para utilizar concentradores o repetidores con el fin de crear los enlaces de la red.

Las reglas para construir de manera correcta segmentos de Fast Ethernet incluyen lo siguiente:

- Limitaciones sobre la longitud máxima de los segmentos que conectan un equipo de terminal de datos (DTE, por sus siglas para Data Terminal Equipment) a un DTE.
- Limitaciones sobre la longitud máxima de segmentos que conectan DTE a un puerto repetidor.

- Limitaciones sobre el diámetro máximo de la red.
- Limitaciones sobre el número máximo de repetidores y la longitud máxima de segmento que conecta los repetidores.

Limitaciones sobre la longitud máxima de los segmentos DTE-DTE

Cualquier fuente de tramas de datos para la red, incluidos los adaptadores de red, puertos de enrutador o puente, módulos de control de redes u otros dispositivos similares, puede desempeñar el papel de DTE. La característica distintiva de un dispositivo DTE es que genera una nueva trama para el segmento compartido. (Aunque los puentes o enrutadores transmiten tramas previamente generadas por adaptadores de red utilizando sus puertos de salida, estas tramas son nuevas para los segmentos de red a los cuales están conectados puertos de salida específicos.) Sin embargo, el puerto repetidor no es un dispositivo DTE, pues repite bit por bit las tramas que han aparecido en el segmento.

En una típica configuración de red Fast Ethernet, varios dispositivos DTE se encuentran conectados a puertos repetidores, formando así una red con una topología de estrella. Las conexiones DTE-DTE no se encuentran en segmentos compartidos (excepto para la exótica configuración en la que los adaptadores de red de dos computadoras están conectados directamente por cable). Por otro lado, para puentes o enrutadores, tales conexiones son bastante normales. En esta situación, un adaptador de red se halla conectado de manera directa al puerto de un dispositivo o estos dispositivos están directamente conectados a otro.

Las longitudes máximas del segmento DTE-DTE de acuerdo con el IEEE 802.3u se proporcionan en la tabla 13.1.

Limitaciones sobre redes Fast Ethernet basadas en repetidores

Los repetidores Fast Ethernet están divididos en dos clases:

- Los **repetidores de clase I** soportan todos los tipos de codificación lógica de datos: 4B/5B y 8B/6T, lo cual significa que permiten traducir códigos lógicos a 100 Mbps. Por esta razón, los repetidores de clase I pueden tener puertos de los tres tipos de capa física: 100Base-TX, 100Base-FX y 100Base-T4.
- Los **repetidores de clase II** soportan 4B/5B o 8B/6T y tienen puertos 100Base-T4 o puertos 100Base-TX y 100Base-FX, pues estas especificaciones de capa física utilizan ambas codificaciones 4B/5B.

En un dominio de colisión puede haber solamente un repetidor de clase I: éste introduce un retardo de propagación de señal significativo, debido a la necesidad de traducir las señales de una codificación lógica a otra. Este retardo es de 70 bt.

TABLA 13.1 Longitudes máximas de segmento DTE-DTE

Estándar	Tipo de cable	Longitud máxima de segmento
100Base-TX	UTP categoría 5	100 m
100Base-FX	Fibra óptica multimodal 62.5/125 µm	412 m (half-dúplex) hasta 2 km (full-dúplex)
100Base-T4	UTP categorías 3, 4 o 5	100 m

TABLA 13.2 Parámetros de redes Fast Ethernet utilizando repetidores de clase I

Tipo de cable	Diámetro máximo de la red (m)	Longitud máxima del segmento (m)
Solamente par trenzado (TX)	200	100
Solamente par trenzado (FX)	272	136
Varios segmentos basados en par trenzado y un segmento basado en fibra óptica	260	100 (TX) 160 (FX)
Varios segmentos basados en par trenzado y varios segmentos basados en fibra óptica	272	100 (TX) 136 (FX)

Los repetidores de clase II introducen un retardo de propagación de señal más pequeño: 46 bt para puertos TX/FX y 33.5 bt para puertos T4. Por lo tanto, el número más grande de dichos repetidores en un dominio de colisión simple es de dos.

La limitación en el número de repetidores de Fast Ethernet no presenta una dificultad seria cuando se construyen redes extensas, porque el uso de switches y ruteadores divide la red en varios dominios de colisión, cada uno de los cuales puede estar basado en uno o dos repetidores. La longitud total de la red en este caso no tendrá limitaciones.

La tabla 13.2 enumera las reglas para construir una red mediante repetidores de clase I.

Tales limitaciones están ilustradas por la configuración típica de red que se muestra en la figura 13.5.

De este modo, la regla de los cuatro concentradores se convierte en la *regla de uno* o *dos concentradores* para Fast Ethernet: el número de concentradores depende del tipo de concentrador.

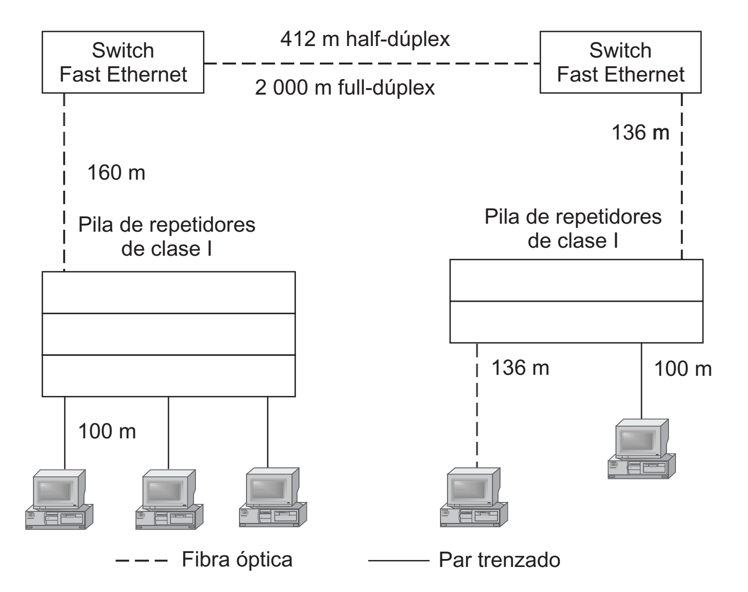


FIGURA 13.5 Ejemplos de redes Fast Ethernet utilizando repetidores de clase I.

Cuando se determina la exactitud de la configuración de la red, en vez de utilizar la regla de uno o dos concentradores, es posible calcular el valor de retardo de trayectoria (PDV, de acuerdo con las siglas de Path Delay Value), como se muestra en el capítulo 12 en el ejemplo para Ethernet de 10 Mbps.

Como con el Ethernet de 10 Mbps, el estándar 802.3 proporciona datos de referencia para calcular el PDV en Fast Ethernet.

13.2.5 Características específicas de 100VG-AnyLAN

Aunque **100VG-AnyLAN** pone en práctica muchas soluciones técnicas avanzadas, no tuvo mucho apoyo y quedó fuera de uso; no encontró su campo de aplicación porque, en comparación con el tradicional y más conveniente Fast Ethernet, probó ser demasiado complicado. Esto se acentúa debido a que Gigabit Ethernet soporta aplicaciones que necesitan altas velocidades de transmisión, lo cual asegura la transmisión de datos a 1 000 Mbps y conserva el vínculo histórico con Ethernet y Fast Ethernet.

En comparación con Fast Ethernet, 100VG-AnyLAN se distingue del Ethernet clásico en un número más significativo de sentidos.

El acceso a un medio compartido se lleva a cabo según el fundamento del método sobre todo diferente: la **prioridad por la demanda**. Este método de acceso está basado en la delegación de funciones de arbitraje hacia el concentrador, lo que resuelve el problema del acceso al medio compartido. Una red 100VG-AnyLAN incluye un **concentrador central** (también conocido como **concentrador raíz**) al que se encuentran conectados los nodos extremos y otros concentradores (figura 13.6).

Se permiten tres niveles en cascada en una red 100VG-AnyLAN. Cada concentrador y adaptador de 100VG-AnyLAN deben configurarse para funcionar con tramas Ethernet o Token Ring. La circulación simultánea de ambos tipos de tramas no está permitida.

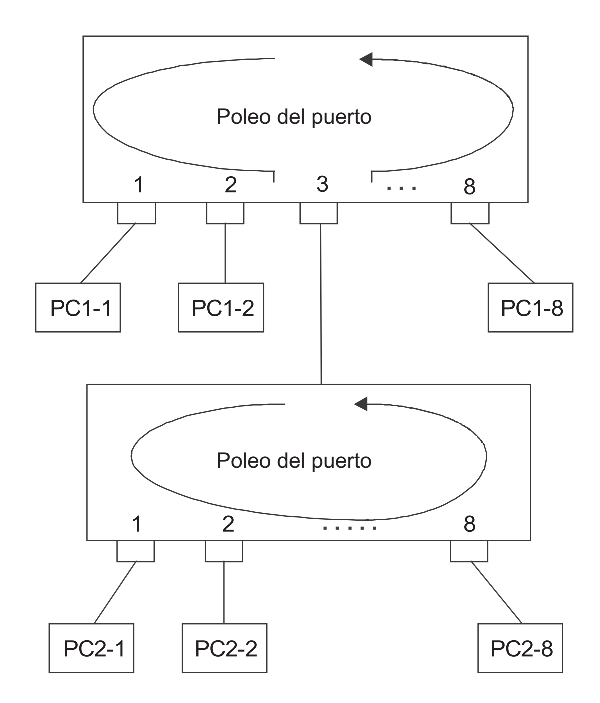


FIGURA 13.6 Red 100VG-AnyLAN.

El concentrador realiza poleo en todos los puertos. Una estación que necesita transmitir un paquete envía una señal especial de baja frecuencia hacia el concentrador, con lo que solicita permiso para transmitir una trama y especificar su prioridad. Las redes 100VG-AnyLAN utilizan dos niveles de prioridad: bajo y alto. La prioridad baja corresponde a los datos normales (servicio de archivo, servicio de impresión, etc.), mientras que la prioridad alta corresponde a los datos sensibles al retraso (como los datos de multimedia). Las prioridades de solicitud tienen componentes estáticos y dinámicos, lo cual significa que una estación de baja prioridad se asignará de manera automática como de prioridad alta si no tiene acceso a la red durante un periodo largo.

Si el medio está disponible, el concentrador permitirá la transmisión del paquete. Después de analizar la dirección de destino del paquete recibido, el concentrador lo envía automáticamente al nodo de destino. Si la red está ocupada, el concentrador colocará la solicitud recibida en la cola, la cual se procesa de acuerdo con el orden de las llegadas de solicitud, según sus prioridades que tengan. Si otro concentrador se conecta al puerto, el poleo se pospone hasta que el concentrador de más bajo nivel completa el poleo. Las estaciones conectadas a concentradores de diferentes niveles jerárquicos no tienen ventajas relacionadas para acceder al medio compartido, pues la decisión de proporcionar el acceso se hace solamente cuando todos los concentradores completan el poleo de todos sus puertos.

Así, ¿cómo sabe el concentrador a qué puerto está conectada la estación de destino? En las otras tecnologías, la trama se transmite a las otras estaciones de la red, y la estación de destino, una vez que ha reconocido su dirección, copia esa trama a su búfer o memoria temporal. Para resolver este problema, el concentrador reconoce la dirección MAC de la estación cuando esa estación está físicamente conectada a la red por el cable. En contraste con las otras tecnologías, en las cuales la conexión física prueba la conectividad del cable (la prueba de la integridad del enlace en 10Base-T) y determina la velocidad de operación del puerto (autonegociación en Fast Ethernet), el concentrador 100VG-AnyLAN determina la dirección MAC de la estación cuando establece una conexión física y la almacena en la tabla de las direcciones MAC (esta tabla es similar a las de puente o enrutador). La diferencia entre los concentradores de 100VG-AnyLAN y los puentes o enrutadores es que los concentradores no tienen un búfer (memoria temporal) interno para almacenar tramas; por lo tanto, reciben sólo una trama desde las estaciones de trabajo en red, la envían al puerto de destino y no reciben nuevas tramas hasta que la trama se recibe en su totalidad en la estación de destino. Esto significa que se protege el efecto de un medio compartido. De esta manera, las mejoras se hallan relacionadas únicamente con la seguridad de la red, pues las tramas no son liberadas a puertos extraños y las hacen más difíciles de detectar.

100VG-AnyLAN soporta diversas especificaciones de capa física. La primera versión estuvo destinada a utilizar cuatro UTP de categorías 3, 4 y 5. Algún tiempo después aparecieron otras variantes, para dos UTP categoría 5, dos STP Tipo 1 o dos fibras ópticas multimodales.

13.3 GIGABIT ETHERNET

PALABRAS CLAVE: grupos de trabajo 802.3z y 802.3ab, Gigabit Ethernet, código 8B/10B, par trenzado de categoría 5, calidad de servicio (QoS), enlaces redundantes, CSMA/CD, fibra óptica, STP, extensión, modo de ráfaga, BurstLength (extensión de ráfaga), 1000Base-SX, 1000Base-LX, 1000Base-CX, código 4B/5B y AM5.

13.3.1 Perspectiva histórica

No mucho después de que aparecieran productos Fast Ethernet en el mercado, los administradores e integradores de redes descubrieron ciertas limitaciones cuando construyeron amplias redes para empresas. En muchos casos, los servidores conectados utilizaban un canal de 100 Mbps para sobrecargar las líneas troncales o backbones FDDI y Fast Ethernet, que también funcionaban a 100 Mbps. Entonces fue evidente la necesidad de contar con la siguiente capa de jerarquía de velocidad. En 1995, velocidades más altas solamente podían ser proporcionadas por switches ATM, los cuales rara vez eran utilizados en LAN debido a sus altos costos y diferencias significativas respecto a las tecnologías LAN clásicas.

Por lo tanto, el siguiente paso de la IEEE fue bastante lógico. En el verano de 1996 se creó el grupo de trabajo 802.3z: fue dirigido a diseñar un protocolo tan próximo a Ethernet como fuera posible, pero suministrando una velocidad de bits de 1 000 Mbps. Como ocurrió con Fast Ethernet, estas noticias fueron recibidas con entusiasmo por los partidarios de Ethernet.

La razón principal para este entusiasmo fue el prospecto de una transición suave de los troncales de red hacia Gigabit Ethernet, de manera semejante a la transición desde los segmentos congestionados de bajo nivel de Ethernet hacia Fast Ethernet. De manera adicional, por ese tiempo ya se había acumulado alguna experiencia de transmisión de datos a velocidades de gigabits. En las MAN y las WAN, esto se consiguió con fundamento en SDH, y en las LAN el mismo objetivo se había logrado con base en un canal de fibra, el cual se utiliza principalmente para conectar dispositivos periféricos de alta velocidad a potentes computadoras. Asimismo, asegura la transmisión de datos sobre cable de fibra óptica a velocidades cercanas a 1 gigabit; para obtener esto, se emplea el código redundante 8B/10B.

El método de codificación 8B/10B utilizado en canal de fibra fue adoptado como la primera versión de la capa física de Gigabit Ethernet.

El estándar 802.3z fue aprobado el 29 de junio de 1998. La tarea de implementar Gigabit Ethernet sobre el fundamento del par trenzado de categoría 5 se delegó al grupo de tarea 802.3ab. Principalmente, esto ocurrió debido a las complicaciones de asegurar las velocidades de transmisión de gigabits empleando este tipo de cable, que en un principio se creó para soportar velocidades de alrededor de 100 Mbps. El grupo de tarea 802.3ab realizó esta labor con éxito y se adoptó pronto el Gigabit Ethernet para un par trenzado de categoría 5.

13.3.2 Problemas

La idea principal de los diseñadores de Gigabit Ethernet fue preservar tanto como fuera posible las ideas del Ethernet clásico mientras se conseguía una velocidad de bits de 1 000 Mbps.

Aunque sería lógico esperar la introducción de innovaciones técnicas que reflejaran las tendencias comunes en la evolución de cualquier nueva tecnología emergente, estas expectativas no fueron satisfechas en el caso de Gigabit Ethernet. En particular, como con sus predecesores de menor velocidad, Gigabit Ethernet *no* soporta las siguientes características para la capa de protocolo:

- Calidad de servicio (QoS)
- Enlaces redundantes
- Prueba de nodos de red y uso del equipo (en el último caso, como con Ethernet 10Base-T, 10Base-F y Fast Ethernet, excepto los enlaces puerto a puerto).

Las tres funciones se ven como promisorias y útiles para las redes contemporáneas y en especial para las redes del futuro cercano. ¿Por qué lo abandonaron los diseñadores de Gigabit Ethernet?

La respuesta es simple. En las LAN de la actualidad se aseguran estas útiles características por medio de switches, los cuales soportan versiones full-dúplex de protocolos de la familia Ethernet. Por lo tanto, los diseñadores de Gigabit Ethernet decidieron que el protocolo básico debe asegurar de manera simple la transmisión rápida de datos, y las funciones más complicadas que no siempre son necesarias (como el soporte QoS) deben delegarse a protocolos de capas superiores que funcionan con switches.

En ese orden de ideas, ¿cuáles características tiene en común Gigabit Ethernet con sus predecesores: Ethernet y Fast Ethernet?

- Se preservan todos los formatos de trama Ethernet.
- La versión half-dúplex del protocolo que soporta CSMA/CD todavía está presente. El mantenimiento de una solución económica con base en un medio compartido permite a Gigabit Ethernet aplicarse en pequeños grupos de trabajo con estaciones de trabajo y servidores rápidos.
- Se soportan todos los tipos principales de cables utilizados en Ethernet y Fast Ethernet, incluidos fibra óptica, par trenzado categoría 5 y STP.

Aunque los diseñadores de Gigabit Ethernet decidieron hacerlo sin construir nuevas características avanzadas, encontraron varios problemas complicados, incluso cuando aseguraban las capacidades funcionales básicas del Ethernet clásico:

- *Asegurar un diámetro de red aceptable para operación con base en un medio compartido*. Debido a las limitaciones impuestas por CSMA/CD sobre la longitud del cable, la conservación del tamaño de la trama y todos los parámetros de CSMA/CD reduciría la longitud de segmento máxima a 25 m para la versión de medio compartido del Gigabit Ethernet. Como muchos campos de aplicación requieren que el diámetro de la red sea por lo menos de 200 m, fue necesario encontrar una solución a este problema sin hacer cambios significativos a Fast Ethernet.
- *Obtener una velocidad de bits de 1 000 Mbps mediante el uso de cable de fibra óptica.* El canal de fibra, que es la capa física que fue tomada como base para la versión de fibra óptica de Gigabit Ethernet, garantiza una velocidad de datos de solamente 800 Mbps.
- *Proporcionar soporte para los cables de par trenzado.* Al principio, este problema parecía no tener solución. Incluso los protocolos de 100 Mbits requieren métodos de codificación más complejos para asegurar que el espectro de señales quepa dentro del ancho de banda del cable.

Para resolver esas tareas, los diseñadores de Gigabit Ethernet tenían que realizar cambios no solamente a la capa física, como fue el caso de Fast Ethernet, sino también a la capa MAC.

13.3.3 Aseguramiento del diámetro de la red de 200 metros

Para extender el diámetro máximo de la red de Gigabit Ethernet a 200 m en modo half-dúplex, los diseñadores siguieron los pasos naturales. Dichas soluciones están basadas en la relación bien conocida (descrita en el “estudio de caso” del capítulo 12) entre el tiempo requerido para transmitir una trama de longitud mínima y el PDV.

El tamaño de trama mínimo fue incrementado (sin tener en cuenta el preámbulo) de 64 a 512 bytes o 4 096 bt. Por consiguiente, el PDV también puede incrementarse a 4 095 bt,

lo que permite un diámetro de la red de aproximadamente 200 m, a condición de que se utilice un repetidor.

Para aumentar la longitud de la trama hasta el valor requerido, el adaptador de red tiene que llenar el campo de datos hasta 448 bytes con una **extensión**, un campo lleno de ceros. Formalmente, el tamaño mínimo de la trama no cambia, pues permanecen 64 bytes de 512 bits. Sin embargo, esto se debe a que el campo *Extensión* está situado después del campo *FCS*. En consecuencia, el valor de este campo no se halla incluido dentro de la suma de verificación y no se tiene en cuenta cuando se especifica la longitud del campo de datos en el campo *Lenght (longitud)*. El campo *Extensión* simplemente rellena la señal portadora, lo cual es necesario para detectar colisiones en forma correcta.

Con el fin de reducir gastos cuando se utilizan tramas demasiado extensas para transmitir reconocimientos o contestaciones breves, los diseñadores estándar permiten que el nodo final transmita varias tramas una después de otra, sin pasar el medio a otras estaciones. Este modo de funcionamiento se conoce como **modo de ráfaga**. La estación puede transmitir varias tramas una tras otra, a condición de que su longitud total no exceda los 65 536 bits u 8 192 bytes. Si la estación necesita transmitir varias tramas pequeñas se le permite hacerlo de ese modo sin rellenar la primera trama hasta 512 bytes al sumar el campo *Extensión*. En este caso, la estación puede transmitir varias tramas de manera secuencial hasta alcanzar el límite de 8 192 bytes (este límite incluye todos los bytes de la trama, entre ellos el preámbulo, el encabezado, los datos y la suma verificadora). El límite de 8 192 bytes se conoce como **BurstLength (longitud de ráfaga)**. Si la estación ha comenzado a transmitir una trama y el límite BurstLength se ha alcanzado en el curso de la transmisión de la trama, se permite a la estación completar la transmisión de aquélla.

Incrementar el tamaño de la trama "combinada" a 8 192 bytes retarda el acceso al medio para otras estaciones; no obstante, a 1 000 Mbps, este retraso no es significativo.

13.3.4 Especificaciones del medio físico 802.3z

El estándar 802.3z define los siguientes tipos de medio físico:

- Cable de fibra óptica en modo simple
- Cable de fibra óptica multimodal 62.5/125
- Cable de fibra óptica multimodal 50/125
- Cable de cobre balanceado con protección (blindaje)

Para transmitir datos sobre el cable de fibra óptica multimodal tradicional, el estándar define el uso de emisores que funcionan a dos longitudes de onda: 1 300 y 850 nm. El uso de LEDs con una longitud de onda de 850 nm se explica como sigue: son bastante más económicos que los LED que funcionan a 1 300 nm. No obstante, se disminuye la longitud máxima de cable, pues la atenuación de la fibra óptica multimodal a una longitud de onda de 850 nm es de más del doble que a 1 300 nm. Sin embargo, el precio menor es muy importante para una tecnología que por lo general es costosa, como lo es Gigabit Ethernet.

Para la fibra óptica multimodal, el estándar 802.3z define las especificaciones siguientes: **1000Base-SX** y **1000Base-LX**.

En el primero de los casos, la longitud de onda es de 850 nm (la letra S proviene del inglés *short wavelength*, es decir, longitud de onda corta); en el segundo caso, es de 1 300 nm (la L es por *long wavelenght*, es decir, longitud de onda larga).

Para 1000Base-LX, la fuente de luz siempre es un LED semiconductor con una longitud de onda de 1 300 nm.

La 1000Base-LX permite usar tanto cable multimodal (longitud máxima de segmento hasta 500 m) como el de modo simple (longitud máxima de segmento según la potencia del transmisor y la calidad del cable, y puede alcanzar varias decenas de kilómetros).

La especificación **1000Base-CX** utiliza cable de cobre balanceado con protección (blindaje) como el medio de transmisión. Este cable tiene una impedancia de 150 ohms. La longitud máxima de segmento es de sólo 25 m, de manera que esta solución es adecuada únicamente para equipo dentro de un solo cuarto.

13.3.5 Gigabit Ethernet basado en un par trenzado de categoría 5

Cada par de categoría 5 tiene un ancho de banda garantizado de 100 MHz. Para transmitir datos con un cable de esta naturaleza a 1 000 Mbps se decidió organizar la transmisión de datos en paralelo empleando los cuatro pares de cables.

Lo anterior redujo la velocidad de transmisión de datos sobre cada par hasta 250 Mbps. Pero, incluso a esta velocidad, fue necesario inventar un método de codificación que asegurara que el espectro no excediera los 100 MHz. Por ejemplo, el código 4B/5B no puede resolver este problema, pues a tal velocidad, la frecuencia de 155 MHz hace la contribución principal al espectro de señales. También debería recordarse que cada nueva tecnología debe soportar no solamente el modo half-dúplex clásico considerado en este capítulo, sino también el modo full-dúplex, que se verá con más detalle en el capítulo 15. Al principio, puede parecer que el uso simultáneo de cuatro pares impide que la red funcione en el modo full-dúplex, puesto que no quedan pares libres para la transmisión bidireccional simultánea de datos de nodo a nodo.

Sin embargo, el grupo de tarea 802.3ab encontró respuestas para este par de preguntas.

Para la codificación de datos se utilizó el código PAM5, que utilizaba cinco niveles de potencial (−2, −1, 0, +1 y +2). Por lo tanto, cada par transmite 2.322 bits de información ($\log_2 5$) por ciclo de reloj, de modo que, para obtener 250 Mbps, la frecuencia de reloj de 250 MHz debe disminuirse 2.322 veces. Los diseñadores del estándar decidieron utilizar una frecuencia algo mayor: 125 MHz. Para esta frecuencia de reloj, PAM5 tiene un espectro más reducido que 100 MHz, lo cual significa que puede transmitirse sin distorsión sobre el cable de categoría 5.

Durante cada ciclo de reloj se transmiten ocho bits de información (más que $2.322 \times 4 = 9.288$), lo cual da una velocidad total de 1 000 Mbps. La transmisión de exactamente ocho bits por cada ciclo de reloj se obtiene debido a que solamente se utilizan 256 ($2^8 = 256$) de las 625 ($5^4 = 625$) combinaciones disponibles del código PAM5. El receptor utiliza las combinaciones restantes para controlar la información recibida y distinguir las combinaciones legítimas del ruido del fondo.

Para organizar el modo full-dúplex, los diseñadores de la especificación 802.3ab aplican la técnica de obtener la señal recibida a partir de la agregada. Dos transmisores funcionan al transmitir información entre ellos en direcciones inversas, empleando cada uno de los cuatro pares en el mismo intervalo de frecuencia (figura 13.7). El diseño del desacoplador híbrido H permite al receptor y transmisor del mismo nodo usar el par trenzado de manera simultánea para transmisión y recepción (de modo semejante a los transceptores utilizados en Ethernet que se basan en cable coaxial).

Para separar la señal recibida de la que el nodo transmite en ese momento, el receptor sustrae su propia señal de la resultante. Desde luego, ésta no es una operación fácil y se requieren procesadores digitales de señales (DSP, por sus siglas para Digital Signal Processors) especiales.

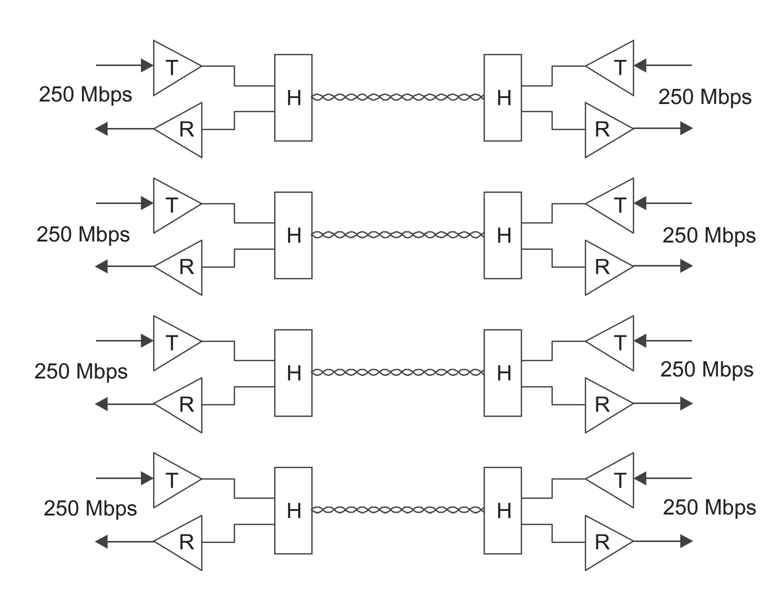


FIGURA 13.7 Transmisión bidireccional utilizando cuatro UTP de categoría 5.

RESUMEN

- La necesidad de contar con una tecnología de alta velocidad pero económica para conectar estaciones de trabajo potentes a una red a principios de la década de 1990, creó una serie de iniciativas que desarrollarían una nueva tecnología tan simple y eficaz como la de Ethernet pero que funciona a 100 Mbps.
- Los especialistas se dividieron en dos grupos, los que finalmente diseñaron dos estándares adoptados en el otoño de 1995: el comité IEEE 802.3 aprobó el estándar Fast Ethernet, que casi duplica el Ethernet de 10 Mbps, y el comité 802.12 especialmente creado adoptó 100VG-AnyLAN, la cual preserva el formato de trama de Ethernet pero modifica de manera significativa el método de acceso.
- Fast Ethernet preservó CSMA/CD, dejando sin cambios su algoritmo de trabajo y parámetros temporales en intervalos de bits (aunque el intervalo de bits disminuyó 90%). Todas las diferencias entre Fast Ethernet y Ethernet clásico se manifiestan en la capa física.
- El estándar Fast Ethernet define tres especificaciones de capa física: 100Base-TX, 100Base-FX y 100Base-T4.
- El diámetro máximo de una red Fast Ethernet es de aproximadamente 200 m; valores más precisos dependen de la especificación del medio físico. En el dominio de colisión de Fast Ethernet no puede haber más de un repetidor de clase I o no más de dos repetidores de clase II.
- El Fast Ethernet basado en un par trenzado permite que dos puertos elijan el modo de operación más eficaz al poner en práctica la autonegociación. Dos puertos pueden elegir entre 10 y 100 Mbps, así como entre el modo half-dúplex y el modo full-dúplex.
- En 100VG-AnyLAN, un concentrador que soporta la prioridad por la demanda desempeña el papel de árbitro y toma una decisión para proporcionar acceso de las estaciones al medio compartido.

- Gigabit Ethernet agrega un nuevo escenario a la jerarquía de velocidades de la familia Ethernet: 1 000 Mbps. Este nivel favorece la construcción eficaz de LAN extensas con servidores y troncales de bajo nivel que funcionan a 100 Mbps a medida que el troncal de Gigabit Ethernet los conecta, asegurando reservas significativas de ancho de banda.
- Los diseñadores de Gigabit Ethernet mantienen una gran continuidad respecto a Ethernet y Fast Ethernet. Gigabit Ethernet utiliza el mismo formato de trama que las versiones anteriores de Ethernet y soporta los modos full-dúplex y half-dúplex, así como CSMA/CD con cambios mínimos.
- El grupo de tarea especial 802.3ab diseñó Gigabit Ethernet para UTP de categoría 5. La transmisión de datos a 1 000 Mbps se asegura por medio de los puntos siguientes:
  - Transmisión simultánea de datos a través de cuatro UTP.
  - Codificación PAM5, asegurando la transmisión de datos a 250 Mbps al usar un par trenzado simple.
  - Transmisión de información simultánea bidireccional en el modo full-dúplex, con separación de la señal recibida respecto a la señal común utilizando DSP especiales.

PREGUNTAS DE REPASO

1. ¿Qué desventajas de CSMA/CD se eliminan mediante la prioridad por la demanda?
2. ¿Por qué los diseñadores de Fast Ethernet decidieron preservar CSMA/CD?
3. ¿Qué topologías son soportadas por una red Fast Ethernet basadas en un medio compartido?
4. ¿Cuál es el diámetro máximo de una red Fast Ethernet?
5. ¿Cuántos pares de cable se utilizan para la transmisión de datos en 100Base-T4?
6. ¿Cuáles son las diferencias entre los repetidores de clase I y de clase II de Fast Ethernet?
7. ¿Por qué solamente se permite un repetidor de clase I en una red Fast Ethernet?
8. ¿Cuál es el valor mínimo de la banda entre paquetes en Gigabit Ethernet?
9. Debido al aumento en el ancho de banda, los diseñadores de Gigabit Ethernet tuvieron que incrementar el tamaño mínimo de trama hasta 512 bytes. Cuando los datos transmitidos no pueden llenar el campo de datos de la trama, se complementa hasta la longitud requerida mediante rellenado, el cual no conduce ninguna información útil. ¿Qué medidas se han tomado en Gigabit Ethernet con el fin de reducir los gastos para la transmisión de datos breves?
10. ¿Qué medidas se han tomado en Gigabit Ethernet para asegurar la transmisión de datos a 1 000 Mbps al usar un par trenzado?

    a) Calidad incrementada de un cable de par trenzado

    b) Uso de cuatro pares de cable en lugar de dos

    c) Aumento en el número de estados del código de señal

    d) Modulación de la Amplitud de la Cuadratura Implementada
11. ¿Por qué Gigabit Ethernet utiliza fibra óptica tanto multimodal como de modo simple?

PROBLEMAS

1. **Tarea:** utilice las tablas 13.3 y 13.4 para determinar qué reserva de estabilidad tiene una configuración de Fast Ethernet con un repetidor de clase I.

TABLA 13.3 Retardos introducidos por el cable

Tipo de cable	Retardo duplicado (intervalo de bit por 1 m)	Retardo duplicado en el cable de máxima longitud
UTP categoría 3	1.14 bt	114 bt (100 m)
UTP categoría 4	1.14 bt	114 bt (100 m)
UTP categoría 4	1.112 bt	111.2 bt (100 m)
STP	1.112 bt	111.2 bt (100 m)
Fibra óptica	1.0 bt	412 bt (412 m)

TABLA 13.4 Retardos introducidos por los adaptadores de la red

Tipo de adaptador de la red	Retardo máximo para el viaje redondo
Dos adaptadores TX/FX	100 bt
Dos adaptadores T4	138 bt
Un adaptador TX/FX y un adaptador T4	127 bt

SUGERENCIA *Cuando se determina la exactitud de una red Fast Ethernet, en vez de aplicar la regla de uno o dos concentradores, es posible calcular el PDV, como se hizo en el "estudio de caso" del capítulo 12 para la red Transmash.*

Como ocurre con Ethernet de 10 Mbps, el estándar Fast Ethernet proporciona datos fuente para calcular la señal PDV. No obstante, la forma de estos datos y el método de cálculo han cambiado. Fast Ethernet proporciona datos en retardos duplicados introducidos por cada segmento de la red, sin dividir los segmentos de ésta en izquierdo, intermedio y derecho. Además, los retardos introducidos por los adaptadores de la red tienen en cuenta los preámbulos de la trama. Por lo tanto, PDV debe compararse con 512 bt (es decir, el tiempo requerido para transmitir una trama de longitud mínima sin un preámbulo).

Para repetidores de clase I, el RTT puede calcularse de la manera siguiente: los retardos introducidos durante la transmisión de la señal al usar el cable se calculan con base en los datos proporcionados en la tabla 13.3, que tiene en cuenta que la señal debe pasar dos veces a través del cable. Los retardos introducidos por dos adaptadores de red (o puertos de los switches) que interactúan a través de un repetidor se muestran en la tabla 13.4.

Como el retardo doble introducido por un repetidor de clase I es de 140 bt, es posible calcular RTT para cualquier configuración de red (considerando las longitudes máximas de los segmentos de cable, proporcionados en la tabla 13.2). Si el valor resultante es menor que 512, de acuerdo con el criterio de detección de colisiones, esta configuración de red es correcta. El estándar 802.3 recomienda asegurar una reserva de 4 bits para un funcionamiento estable de la red, pero permite elegir un valor entre 0 y 5 bits.

14

LAS LAN DE MEDIOS COMPARTIDOS

DESCRIPCIÓN DEL CAPÍTULO

14.1 INTRODUCCIÓN

En este capítulo se estudian diversas tecnologías LAN de medios compartidos además de Ethernet. Dicha lista incluye Token Ring y FDDI, los cuales fueron utilizados con éxito durante largo tiempo en las LAN que requerían rendimiento y confiabilidad superior, además de ser un área de cobertura incrementada. Antes de la llegada de las LAN conmutadas, estas tecnologías superaban a Ethernet en tales aspectos. Debido a ello, se les dio preferencia al construir troncales de LAN o al crear redes para organizaciones financieras o gubernamentales, es decir, donde el rendimiento y la confiabilidad eran de importancia fundamental. Token Ring y FDDI emplean un método de acceso determinista, permiten compartir de manera más eficaz el medio de transmisión e incluso proporcionan soporte QoS para tráfico en tiempo real.

Token Ring y FDDI utilizan la topología de anillo de enlaces físicos, los cuales habilitan para controlar la funcionalidad de la red en forma automática. Las redes FDDI aseguran además la recuperación automática de la red después de las fallas. Para proporcionar esto utilizan un anillo doble con el fin de conectar los nodos; en ese aspecto son semejantes a las redes SDH.

Los medios de comunicaciones inalámbricos, por su naturaleza física, son compartidos. En este capítulo se estudian dos tecnologías inalámbricas: IEEE 802.11 y Bluetooth (IEEE 802.15.1). La primera permite crear LAN inalámbricas y la última está relacionada con las redes de área personal (PAN). Cada tecnología tiene sus métodos de acceso al medio.

14.2 TOKEN RING

PALABRAS CLAVE: Token Ring, monitor activo, tiempo de retención de la señal, liberación temprana de la señal, prioridad, procedimiento de señal circulante, unidad de acceso a estación múltiple (MAU o MSAU, por sus siglas para MultiStation Access Unit), concentrador pasivo, concentrador activo, STP Tipo I, UTP Tipo 3, UTP Tipo 6, tipos de sistema de cableado IBM y cable de fibra óptica.

La tecnología **Token Ring** fue diseñada por IBM en 1984 y posteriormente pasó al Comité IEEE 802 como un proyecto estándar propuesto. Dicho comité utilizó esta tecnología como un fundamento para el estándar 802.5, el cual fue adoptado en 1985. Durante largo tiempo, IBM empleó Token Ring como su principal tecnología de redes para construir LAN basadas en diferentes clases de computadoras, desde supercomputadoras ("mainframes") y poderosas minicomputadoras hasta las PC. Sin embargo, en años recientes, la familia Ethernet ha dominado incluso entre los productos de IBM.

Las redes Token Ring funcionan a dos velocidades de bits: 4 y 16 Mbps. No se permiten estaciones de trabajo que funcionen a diferentes velocidades dentro de un anillo simple. Las redes Token Ring que funcionan a 16 Mbps incluyen algunas mejoras sobre el algoritmo de acceso estándar empleado en las redes de 4 Mbps.

Token Ring es más complejo que Ethernet y proporciona algunas características básicas para la tolerancia a las fallas. En una red Token Ring se definen procedimientos especiales para controlar el funcionamiento de la red, los cuales aplican la propiedad de retroalimentación inherente a la topología de anillo: la trama enviada siempre regresa al remitente. En algunos casos, los errores de la red se corrigen de manera automática; por ejemplo, una señal perdida puede ser restablecida. En otros casos, la red solamente informa de los errores detectados y el personal de soporte debe eliminarlos en forma manual.

Para controlar el funcionamiento de la red, una de sus estaciones de trabajo es responsable de asumir el papel de **monitor activo**, el cual se elige durante el inicio del anillo. El valor máximo de la dirección del control de acceso al medio (MAC) es el criterio. Si el monitor activo falla, se repite el procedimiento de inicio del anillo y se selecciona un nuevo monitor activo. Con el fin de habilitar las redes para detectar la falla del monitor activo, éste genera una trama especial que notifica a las otras estaciones de trabajo de su presencia. Ello ocurre cada 3 segundos (siempre que el monitor activo esté en funcionamiento). Si una trama de dicha clase no es enviada por más de 7 segundos, otras estaciones de trabajo iniciarán el procedimiento de seleccionar un nuevo monitor activo.

14.2.1 Acceso a la señal circulante (Token-Passing)

Las redes Token Ring utilizan el medio compartido basadas en el principio de acceso a la señal circulante descrito en el capítulo 12 cuando se explican las funciones de la capa MAC. Se describirán con más detalle algunos aspectos específicos de este método, lo cual es característico de la tecnología **Token Ring de 4 Mbps** detallada en el estándar 802.5.

En una red Token Ring, cada estación recibe los datos directamente de sólo una estación: la que está antes de ella en el anillo. Cada estación transmite los datos al vecino siguiente más cercano en el anillo.

Una vez recibida la señal, la estación la analiza. Si dicha estación no tiene datos para transmitir, pasará la señal a la siguiente estación. Cuando la señal se pasa a una estación que tiene datos para la transmisión, retira la señal del anillo, lo cual le facilita tener acceso al medio físico para transmitir sus datos. Después de eso, la estación envía de manera secuencial una trama de formato especial dentro del anillo, misma que contiene direcciones de inicio y de destino.

Los datos que se transmiten siempre viajan a lo largo del anillo en una dirección, de estación en estación. Todas las estaciones en el anillo retransmiten la trama bit por bit y actúan como repetidores. Si la trama llega al nodo de destino, tal estación reconoce su dirección, copia la trama en su búfer o memoria temporal interna e inserta el indicador de reconocimiento de recepción, o acuse de recibo, en la trama. La estación que envió la trama de datos en el anillo, una vez que la ha recibido de nuevo con el acuse de recibo, retira la trama del anillo y pasa una nueva señal en las redes, permitiendo así a otras estaciones que transmitan datos.

La figura 14.1 contiene un diagrama de tiempo que ilustra el algoritmo de acceso al medio descrito aquí. Muestra el paso del paquete A desde la estación 1 hasta la 3 en un anillo que consta de seis estaciones. Después de que el paquete A pasa al nodo de destino, la estación 3, se establecen dos banderas en este paquete: la bandera de reconocimiento de dirección A y el indicador C, que especifica que el paquete ha sido copiado en el búfer interno. (En la ilustración, esto se representa mediante un asterisco dentro del paquete.) Cuando el paquete regresa a la estación 1, el remitente reconoce su paquete mediante la dirección de inicio y retira el paquete del anillo. Las banderas establecidas por la estación 3 notifican al remitente que el paquete ha sido entregado con éxito a su nodo de destino y copiado en su búfer interno.

El tiempo durante el cual el medio compartido se monopoliza en las redes Token Ring está limitado por un valor fijo, conocido como **tiempo de retención de la señal**. Cuando este tiempo finaliza, la estación debe detener la transmisión de sus datos (se permite completar la transmisión de la trama actual) y pasa la señal a lo largo del anillo. Mientras se retiene la señal, la estación puede transmitir una o más tramas, lo cual depende del tamaño de aquélla y de la duración del intervalo de retención de señal. De manera predeterminada, el tiempo de retención de señal se establece por lo general a 10 mseg; el tamaño máximo de la trama

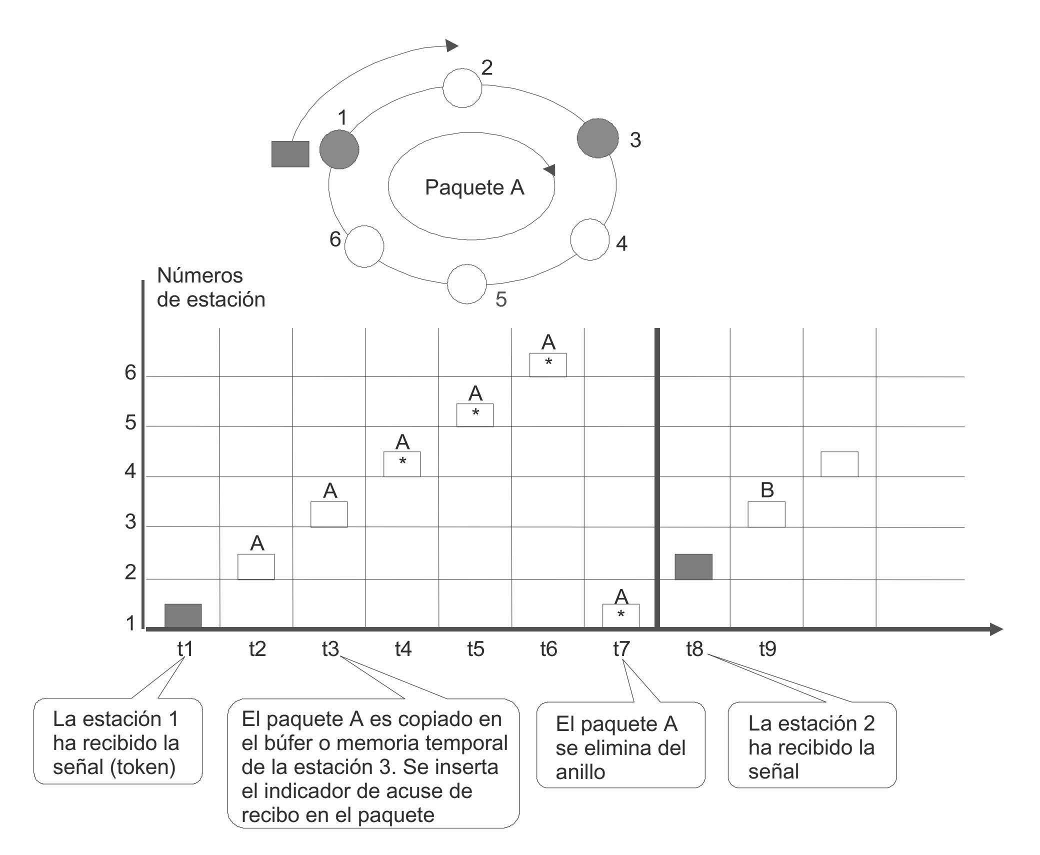


FIGURA 14.1 Acceso a la señal circulante (Token-Passing).

no está definido de modo estricto en el estándar 802.5. Como regla, para redes de 4 Mbps, es de 4 KB; para redes de 16 Mbps, normalmente es de 16 KB. Esos valores fueron seleccionados debido a que, durante el tiempo de retención de señal, la estación debe transmitir por lo menos una trama. A 4 Mbps, es posible transmitir 5 000 bytes durante 10 mseg; a 16 Mbps es posible transmitir 20 000 bytes durante el mismo tiempo. Los tamaños máximos de trama se eligen para tener cierta reserva.

Las redes **Token Ring de 16 Mbps** utilizan un algoritmo de acceso al anillo ligeramente distinto, conocido como **liberación temprana de la señal**. De acuerdo con este algoritmo, la estación pasa la señal de acceso a su siguiente *vecino más cercano en el anillo inmediatamente después de que complete la transmisión del último bit de la trama,* sin esperar que regrese esta última con los bits de acuse de recibo A y C establecidos. En este caso, el ancho de banda del anillo se utiliza con más eficacia, pues las tramas de varias estaciones de trabajo se trasladan a lo largo del anillo de manera simultánea. No obstante, en cualquier momento, sólo una estación de trabajo puede generar tramas: la que tiene la señal de acceso. Las otras estaciones de trabajo en ese momento sólo repiten las tramas transmitidas por otros nodos, de modo que se mantiene el principio de compartir la sesión del tiempo. En este caso, sólo se acelera el procedimiento de circulación de la señal.

Para los diferentes tipos de mensajes se pueden asignar diversas *prioridades* a las tramas transmitidas, desde el 0 (la prioridad más baja) hasta el 7 (la prioridad más alta). La estación de trabajo transmisora decide la prioridad de una trama específica. El protocolo Token Ring recibe este parámetro utilizando interfaces de servicio desde los protocolos de capas superiores, tales como los protocolos de la capa de aplicación. La señal siempre tiene

algún nivel actual específico de prioridad. A su vez, la estación tiene el derecho a capturar la señal transmitida hacia ella sólo si la prioridad de la trama que tiene que transmitir es igual o superior a la prioridad de la señal. De otro modo, la estación tiene que pasar la señal a la siguiente estación a lo largo del anillo.

El monitor activo es el responsable de la presencia de una sola copia de la señal en las redes. Si el monitor activo no recibe la señal durante cierto tiempo (por ejemplo, 2.6 segundos), generará una nueva señal.

El acceso de prioridad en Token Ring está destinado a soportar los requerimientos QoS para las aplicaciones. No obstante, los diseñadores de aplicaciones destinadas para las LAN nunca utilizan esta capacidad.

14.2.2 Capa física de Token Ring

El estándar Token Ring diseñado por IBM atendió en principio las necesidades de los enlaces de redes en edificios al usar concentradores de **unidad de acceso a estaciones múltiples** (**MAU** o **MSAU**, por sus siglas en inglés para **MultiStation Access Unit**), es decir, dispositivos de acceso a estaciones múltiples (figura 14.2). Una red Token Ring puede incluir 260 nodos. El uso de concentradores proporciona a las redes Token Ring una topología física de "estrella"; su topología lógica es un anillo.

Un concentrador Token Ring puede ser activo o pasivo. El **pasivo** simplemente conecta puertos por medio de enlaces internos de modo que las estaciones conectadas a esos puertos puedan formar un anillo. Un concentrador pasivo MSAU no amplifica o vuelve a sincronizar señales. Un dispositivo así puede ser visto como una simple unidad cruzada con una excepción: la MSAU asegura que un puerto específico sea desviado si la computadora conectada a ese puerto es desactivada o apagada. Esto se requiere para asegurar la independencia de la conectividad del anillo respecto al estado de las computadoras conectadas. Por lo regular, la desviación del puerto utiliza circuitos de relevo alimentados por una corriente directa desde el adaptador de la red. Cuando este adaptador se apaga, los contactos de relevo, que por lo regular se encuentran cerrados, conectan la entrada del puerto a sus salidas.

Un **concentrador activo** lleva a cabo funciones de regeneración de la señal; por lo tanto, en ocasiones se conoce como repetidor.

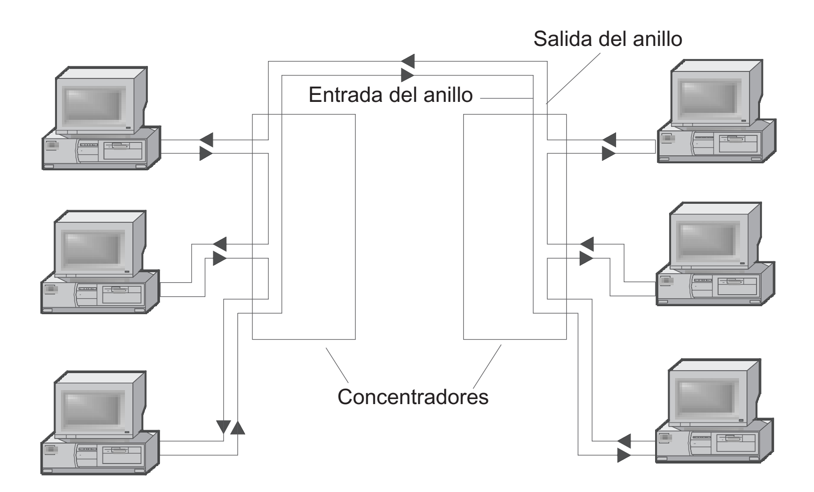


FIGURA 14.2 Configuración física de una red Token Ring.

Si el concentrador es un dispositivo pasivo, ¿cómo puede asegurar la transmisión de la señal de alta calidad sobre distancias considerables, como con las redes a larga escala compuestas de cientos de computadoras? La respuesta es simple. En este caso, cada adaptador de red desempeña el papel de amplificador de la señal; a su vez, la función de la unidad de sincronización se delega al adaptador de la red del monitor activo del anillo. Cada adaptador de red de Token Ring tiene una unidad repetidora capaz de regenerar y sincronizar señales. Sin embargo, este último papel lo lleva a cabo únicamente la unidad repetidora del monitor activo.

En general, una red Token Ring tiene una configuración combinada estrella-anillo. Los nodos extremos están conectados a la MSAU de acuerdo con la topología de estrella, y los concentradores MSAU se encuentran conectados entre si utilizando puertos especiales de anillo de entrada y salida para formar un anillo físico troncal.

Token Ring permite usar varios tipos de cable para conectar concentradores y nodos extremos: STP Tipo 1, UTP Tipo 3 y UTP Tipo 6 (tipos de sistema de cableado IBM), además de cable de fibra óptica.

Cuando se utiliza STP Tipo 1 de la familia de cableado IBM, es posible conectar hasta 260 estaciones de trabajo al anillo, con la longitud máxima de los cables del lóbulo a 100 m. Si se usa un par trenzado sin protección (sin blindaje), el número máximo de estaciones de trabajo se reducirá a 72 y la longitud del cable a 45 m.

La distancia entre los concentradores pasivos MSAU puede alcanzar los 100 m cuando se utiliza cable STP Tipo 1. Cuando se emplea cable UTP Tipo 3, esta distancia se reduce a 45 m. La distancia máxima entre concentradores activos MSAU es de 730 o 365 m, lo cual depende del tipo de cable.

La longitud máxima de anillo de una red Token Ring es de 4 000 m.

NOTA: *Las limitaciones sobre la longitud máxima de anillo y el número de estaciones de trabajo dentro del anillo en Token Ring no son tan restrictivas como las limitaciones en Ethernet. En Token Ring, las restricciones están relacionadas con el tiempo de circulación de la señal a lo largo del anillo, aunque existen consideraciones adicionales que definen la selección de las limitaciones. Por ejemplo, considere que el anillo consta de 260 estaciones de trabajo. Con un tiempo de retención de la señal de 10 milisegundos, en el peor de los casos, la señal regresará al monitor activo después de 2.6 segundos. Este tiempo es igual a la pausa para el viaje redondo de la señal. Principalmente, todos los valores de pausa para los adaptadores de la red de los nodos de la red son ajustables en las redes Token Ring; por lo tanto, es posible construir una red Token Ring con un número más grande de estaciones de trabajo y un anillo más extenso.*

14.3 FDDI

PALABRAS CLAVE: FDDI (Fiber Distributed Data Interface, interfaz de datos distribuidos por fibra), cable de fibra óptica, NRZI, anillo primario o principal, modo thru, anillo secundario, modo envolvente, método de señal circulante, administración de estación (SMT, Station Management), tolerancia a las fallas, conexión dual (DA, Dual Attachment), estación de conexión dual (DAS, Dual Attachment Station), concentrador de conexión dual (DAC, Dual Attachment Concentrator), conexión simple (SA, Single Attachment), estación de conexión simple (SAS, Single Attachment Station), concentrador de conexión simple (SAC, Single Attachment Concentrator), conmutadores de desviación ópticos y buscador dual.

FDDI —Interfaz de datos distribuidos por fibra— fue la primera tecnología LAN que utilizó el cable de fibra óptica como medio de transmisión. Las investigaciones para crear dispositivos y tecnologías para LAN que utilizan enlaces de fibra óptica comenzaron en la década de 1980, poco después de que tales enlaces encontraron su aplicación en las WAN. De 1986 a 1988, el grupo de investigación X3T9.5 de la ANSI desarrolló la primera versión del estándar FDDI, asegurando una transmisión de tramas de 100 Mbps por medio de un anillo dual de fibra óptica de hasta 100 km de largo.

14.3.1 Características principales de FDDI

FDDI está basado en muchos aspectos en Token Ring y ha desarrollado y mejorado sus ideas principales. Los diseñadores de FDDI tienen los siguientes objetivos principales:

- Velocidad de bits incrementada para una transmisión de datos hasta de 100 Mbps.
- Tolerancia a las fallas de la red mejorada mediante la inclusión de procedimientos estándar para la recuperación después de fallas, como pueden ser deficiencias en el cable, funcionamiento incorrecto de un nodo o un concentrador y alto nivel de ruido en la línea.
- Asegurar un nivel máximo de uso potencial de ancho de banda de la red tanto para tráfico asincrónico como sincrónico (sensible al retardo).

> Las redes FDDI se construyen con base en dos anillos de fibra óptica que forman las trayectorias principal y de protección para la transmisión de datos entre nodos de la red. La disponibilidad de los dos anillos es el método principal para mejorar la tolerancia a las fallas en las redes FDDI.

Los nodos críticos que necesitan beneficiarse de este potencial mejorado de tolerancia a las fallas deben estar conectados a ambos anillos. Para transmitir los datos utilizando fibras ópticas, FDDI implementa la codificación lógica 4B/5B con línea de codificación de no retorno a cero con unos invertidos (NRZI). Este método transmite la señal usando un enlace de comunicaciones con una frecuencia de reloj de 125 MHz.

En el modo normal de operación, los datos transmitidos pasan los nodos y las secciones únicamente del **anillo primario**. Este modo se conoce como **modo thru** (es decir, modo de tránsito). El **anillo secundario** no se utiliza en dicho modo.

Si ocurre una falla y parte del anillo primario no puede transmitir los datos (esto puede ser causado por la ruptura del cable o la falla del nodo), el anillo primario se incorporará al anillo secundario (figura 14.3) y formará una vez más un anillo cerrado. Este modo de funcionamiento de la red se conoce como **modo envolvente**. La operación de envoltura se lleva a cabo por medio de concentradores FDDI, adaptadores de redes o ambos. Para simplificar este procedimiento, la transmisión de datos a lo largo del anillo primario o principal siempre es unidireccional (en los diagramas, esto siempre es en el sentido contrario al de las manecillas del reloj). La transmisión de datos a lo largo del anillo secundario va en dirección inversa (en dirección de las manecillas del reloj). Por lo tanto, cuando se forma un anillo común fuera de los dos anillos, los transmisores de las estaciones de trabajo permanecen conectados a los receptores de las estaciones de trabajo vecinas y permiten la transmisión y recepción correctas de la información.

Los estándares FDDI ponen atención en los procedimientos que facilitan que una falla del equipo de la red sea detectada y que se lleve a cabo la reconfiguración requerida. FDDI complementa los mecanismos de detección de fallas de Token Ring al reconfigurar las tra-

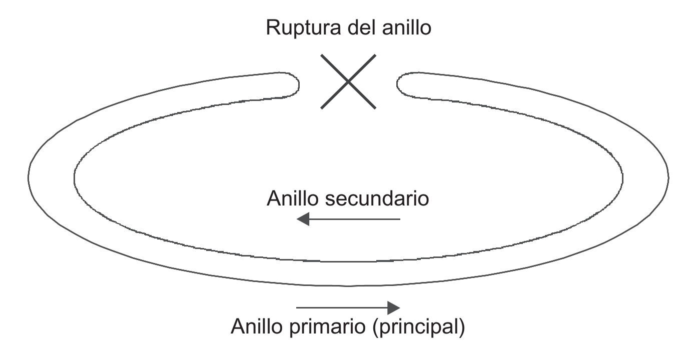


FIGURA 14.3 Reconfiguración de anillos FDDI después de una falla.

yectorias de transmisión de datos con base en enlaces de reserva asegurados por el anillo secundario.

> Las redes FDDI pueden restablecer el uso después de la falla de elementos individuales. En el caso de fallas múltiples, la red se descompone en varias redes autónomas, que no están conectadas entre sí.

Los anillos en FDDI son vistos como un medio compartido simple para la transmisión de datos, de manera que fue desarrollado un método de acceso especial. Éste es parecido al método de acceso de las redes Token Ring y también se denomina **método de señal circulante**. Las estaciones de trabajo FDDI utilizan el mecanismo inicial de liberación de señal, semejante al mecanismo utilizado por la redes Token Ring de 16 Mbps.

Las diferencias en los métodos de acceso Token Ring y FDDI son las siguientes:

- En contraste con Token Ring, el tiempo de retención de la señal no es una constante en las redes FDDI; por el contrario, este tiempo depende de la carga del anillo. Cuando dicha carga es baja, el tiempo de retención de la señal se incrementa, pero durante periodos de congestión puede descender hasta cero. Estos cambios en el método de acceso se relacionan solamente con el tráfico asincrónico, el cual no es sensible a pequeños retardos en la transmisión de la trama. Para el tráfico sincrónico, el tiempo de retención de la señal permanece fijo.
- Un mecanismo de prioridad de la trama similar al de Token Ring no está implementado en FDDI. Los diseñadores decidieron que dirigir el tráfico en ocho niveles de prioridad es redundante y que es suficiente dividir todo el tráfico en dos clases: asincrónico y sincrónico. Este último sirve incluso cuando el anillo está sobrecargado.

En los demás aspectos, enviar tramas entre las estaciones de trabajo del anillo y la capa MAC corresponde a Token Ring.

La figura 14.4 muestra la correspondencia de la pila de protocolo FDDI con el modelo OSI de siete capas. FDDI define el protocolo de capa física y el protocolo de la subcapa MAC de la capa de enlace de datos. Como en muchas otras tecnologías LAN, la tecnología FDDI utiliza el protocolo que controla de enlace lógico (LLC, siglas de Logical Link Control) definido en el estándar IEEE 802.2.

La característica distintiva en la tecnología FDDI es la capa de **administración de estación (SMT)**, la cual lleva a cabo todas las funciones relacionadas con la administración y



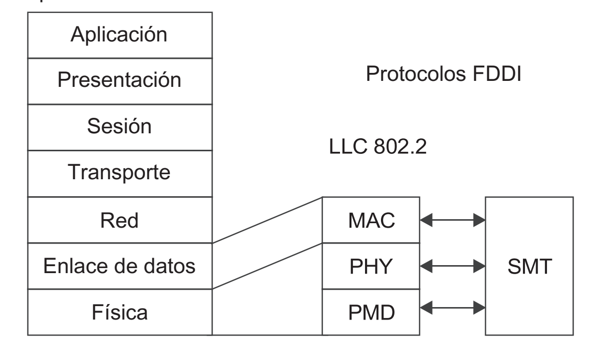


FIGURA 14.4 Pila de protocolo FDDI.

el monitoreo de las demás capas de la pila de protocolo FDDI. Cada nodo de la red FDDI participa en el control del anillo; por lo tanto, todos los nodos intercambian tramas SMT especiales para controlar la red.

Los protocolos de otras capas también participan en asegurar la tolerancia de fallas en las redes FDDI. Por ejemplo, la capa física elimina las fallas de la red por razones físicas, como ruptura de cable. Por otra parte, la capa MAC ayuda a compensar las fallas de la red lógica, como la pérdida de la trayectoria interna requerida para hacer circular la señal y las tramas entre los puertos del concentrador.

14.3.2 Tolerancia a las fallas FDDI

Para asegurar la tolerancia a las fallas, el estándar FDDI proporciona dos anillos de fibra óptica: primario y secundario.

El estándar FDDI define dos tipos de nodos extremos: **estaciones** y **concentradores**. Para conectar las estaciones y concentradores a la red puede utilizarse uno de los métodos siguientes:

- **Conexión dual (DA):** la conexión simultánea tanto al anillo primario como al secundario. La estación y concentrador conectados al usar este método se denominan **estación de conexión dual** (**DAS**) y **concentrador de conexión dual** (**DAC**), respectivamente.
- **Conexión simple** (**SA**)**:** conexión únicamente al anillo primario. La estación o concentrador conectados al emplear este método se llaman **estación de conexión dual** (**SAS**) y **concentrador de conexión simple** (**SAC**), respectivamente.

Por lo regular, aunque no de manera necesaria, los concentradores son DA y las estaciones son SA, como se muestra en la figura 14.5. Para simplificar la conexión de los dispositivos a la red, sus conectores están marcados. Los conectores de tipos A y B deben hallarse en los dispositivos con conexión dual; el conector *maestro* (M) debe estar en concentradores para una conexión simple de la estación, los cuales deben tener un conector de respuesta *esclavo* de tipo S.

En el caso de una ruptura de cable simple entre dispositivos con una conexión dual, una red FDDI puede continuar su funcionamiento normal mediante una reconfiguración automática de las trayectorias internas de transmisión de trama entre los puertos del concentrador (figura 14.6).

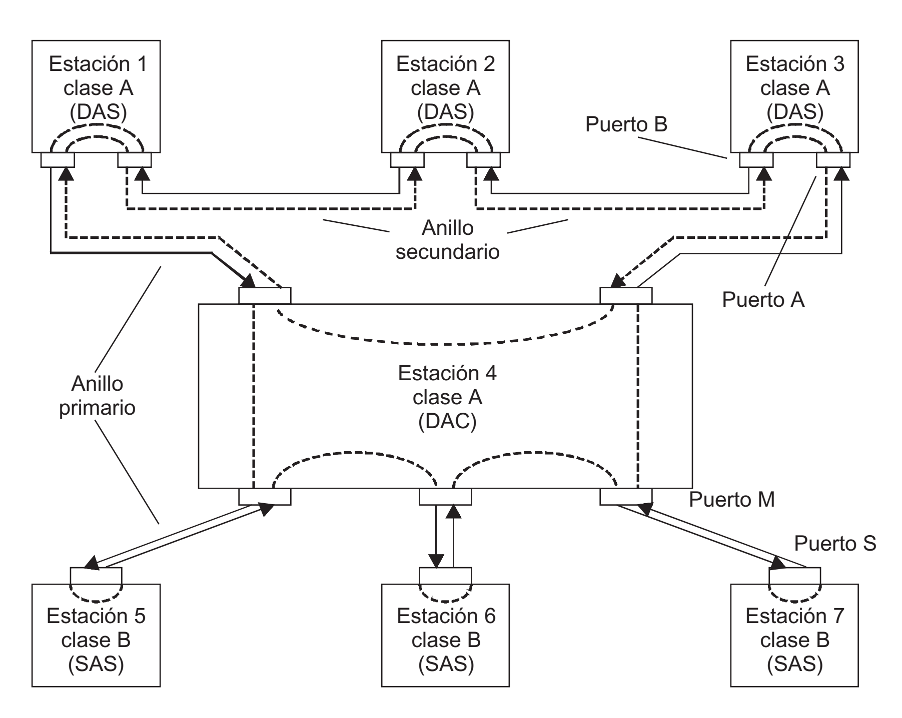


FIGURA 14.5 Conexión de los nodos a anillos FDDI.

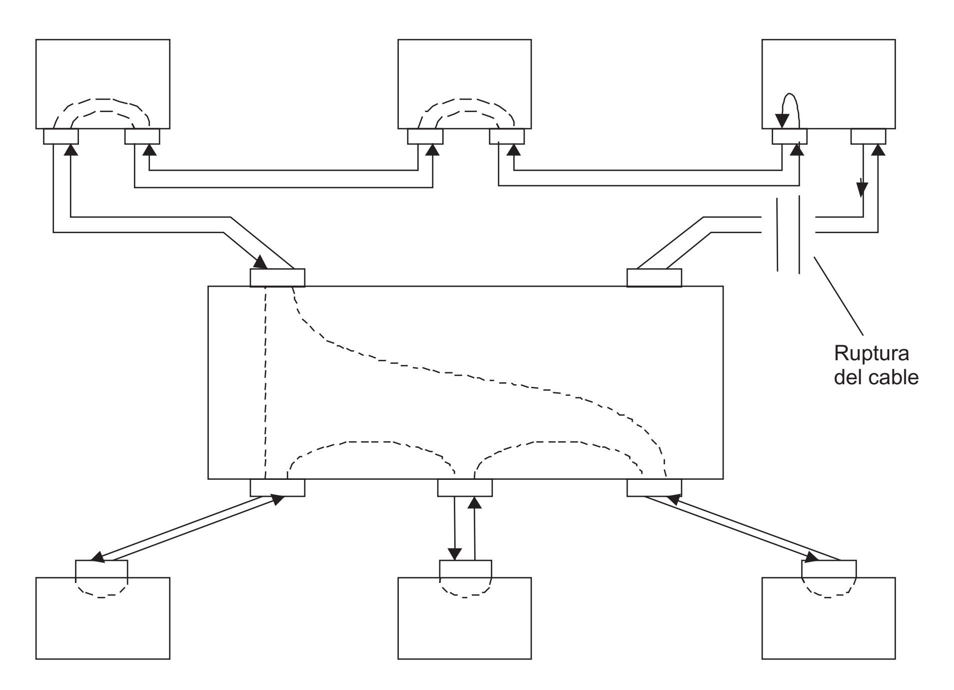


FIGURA 14.6 Reconfiguración de una red FDDI después de una ruptura del cable.

La ruptura del cable doble creará dos redes aisladas FDDI. Cuando un cable que conecta una estación con conexión simple se rompe, esa estación se aísla de la red, pero el anillo continúa en funcionamiento al reconfigurarse las trayectorias internas dentro del concentrador: el puerto M, al cual estaba conectada esa estación, será excluido de la trayectoria común.

Con el fin de preservar la capacidad de la red para funcionar con estaciones de conexión dual (es decir, DAS) que están apagadas, esas estaciones deben hallarse equipadas con **conmutadores de desviación ópticos**, los cuales crean una desviación para rayos luminosos cuando se presentan las interrupciones de energía.

Finalmente, DAS o DAC pueden estar conectadas a dos puertos M de uno o dos concentradores y crear así una estructura de árbol con enlaces principal y de reserva. De manera predeterminada, el puerto B soporta el enlace principal, mientras que el puerto A está destinado a soportar un enlace de reserva. Dicha configuración se conoce como **buscador dual**.

La capa SMT de estaciones de trabajo y concentradores soporta tolerancia a las fallas tanto al rastrear de manera constante los espacios de tiempo de circulación de señales y tramas como al verificar la presencia de conexiones físicas entre puertos vecinos en la red. Las redes FDDI no tienen un monitor activo dedicado, mientras que todas las estaciones y concentradores tienen iguales derechos, y cualquiera de ellos puede iniciar la reinicialización y reconfiguración de la red si se detectan desviaciones de su comportamiento normal.

La reconfiguración de las trayectorias internas en los concentradores y adaptadores de red se lleva a cabo mediante conmutadores ópticos especiales, los cuales redirigen el haz de luz y tienen una estructura más complicada.

La longitud total máxima de un anillo FDDI es de 100 km, en tanto que el número máximo de estaciones de conexión dual en un anillo es de 500.

FDDI fue diseñado para usarlo en segmentos de red críticos (conexiones troncales entre redes extensas, como redes en edificios), además de conectar servidores de alto rendimiento a la red. Por lo tanto, la lista de sus objetivos más importantes incluye asegurar la transmisión de datos de alta velocidad, tolerancia de fallas a nivel de protocolo y distancias extensas entre nodos de la red. Todos estos objetivos fueron alcanzados. Como resultado, FDDI garantiza alta calidad, pero es bastante costoso. Incluso la llegada de una versión más económica basada en cableado trenzado no tuvo una reducción significativa en el costo de conectar un nodo simple a una red FDDI. Por consiguiente, el principal campo de aplicación de FDDI es en troncales de redes que conectan varios edificios, así como MAN de grandes ciudades.

14.4 LAS LAN INALÁMBRICAS

PALABRAS CLAVE: ruido externo, espectro extendido, corrección de errores por adelantado (FEC, Forward Error Correction), terminal oculta, depresión y prevención de colisiones, poleo, estación base, acceso residencial y móvil, redes celulares móviles 3G y 2G, IEEE 802.11, 802.11a, 802.11b, 802.11g, ondas infrarrojas, intervalos de microondas, manipulación por código complementario (CCK, Complementary Code Keying), conjunto básico de servicios (BSS, Basic Service Set), conjunto extendido de servicios (ESS, Extended Service Set), punto de acceso (AP, Access Point), servicios de distribución del sistema (DSS, Distribution System Service), función distribuida de coordinación (DCF, Distributed Coordination Function), función de punto de coordinación (PCF, Point Coordination Function), portal, ventana de contención, coordinador de punto (PC, Point Coordinator), periodo libre de contención, y privacía alámbrica equivalente (WEP, Wired Equivalent Privacy).

14.4.1 Características específicas de las LAN inalámbricas

Las LAN inalámbricas se consideran ahora un complemento de las LAN alámbricas, más que una solución competitiva; sin embargo, las LAN inalámbricas no siempre fueron vistas de esta manera. A mediados de la década de 1990, era popular otra visión: se predijo que con el transcurso del tiempo, más LAN se cambiarían a las tecnologías inalámbricas. La ventaja de las LAN inalámbricas es evidente: son mucho más fáciles de desplegar y actualizarse, porque no es necesaria una voluminosa infraestructura de cable. La movilidad del usuario asegurada es otra ventaja, pero las LAN inalámbricas tienen muchos problemas provocados por el uso de medios inalámbricos inestables e impredecibles. En el capítulo 8 se estudian las características específicas de la propagación de la señal en un medio de esta clase.

El **ruido externo** proveniente de diversos aparatos domésticos, de otros sistemas de telecomunicaciones, del ruido atmosférico y de los reflejos de señal crea dificultades significativas para la recepción confiable de la información. Las LAN están destinadas principalmente a la conexión de computadoras dentro de edificios, y la propagación de una señal de radio dentro de un edificio es mucho más complicada que en exteriores. El estándar IEEE 802.11 proporciona un diagrama de la distribución de la intensidad de señal "para una habitación cuadrada simple con un escritorio de metal estándar y una entrada abierta" (figura 14.7). El estándar hace énfasis en que esta distribución es estática; en realidad, el patrón cambia de manera dinámica. De este modo, el movimiento de diversos objetos dentro de una habitación puede cambiar de manera significativa la distribución de la señal.

Los métodos de *espectro extendido* permiten reducir el ruido que afecta a la señal útil. Aparte de esto, las redes inalámbricas utilizan ampliamente métodos y protocolos de *corrección de errores por adelantado* (FEC) que aseguran la retransmisión de las tramas perdidas; no obstante, la práctica ha demostrado que cuando nada impide a una organización utilizar una LAN cableada, la mayoría prefiere una red así aun cuando sea imposible de efectuar sin un sistema de cableado.

La distribución desigual de la intensidad de la señal produce no sólo errores de bits en la información que se transmite, sino también *incertidumbre de la zona de cobertura de una LAN inalámbrica*. En las LAN cableadas no existe tal problema, pues todos los dispositivos conectados al sistema cableado de un edificio o campus reciben señales y participan en el funcionamiento de la LAN. Las LAN inalámbricas no tienen un área determinada de cobertura: la notación comúnmente adoptada que representa el área como un círculo o un hexágono no es más que una abstracción. En realidad, en algunas partes de una zona de cobertura regular de este tipo, la señal puede ser tan débil que los dispositivos localizados dentro de esos límites pueden ser incapaces de recibir o transmitir información.

El patrón mostrado en la figura 14.7 ilustra bien una situación así. Es necesario destacar que con el transcurso del tiempo, el patrón de distribución de la señal puede cambiar de manera bastante significativa, en cuyo caso la estructura de la LAN se modificará en consecuencia. Debido a esto, incluso los nodos fijos de la red (no destinados a ser móviles) deben tener en cuenta que la LAN inalámbrica no está completamente conectada. Aun si se supone que la señal sea idealmente omnidireccional, las señales de radio se debilitaran de manera proporcional al cuadrado de la distancia a partir de su fuente, lo que puede evitar la creación de una topología completamente conectada. Por lo tanto, sin una estación base, algunos pares de nodos de red no podrán comunicarse simplemente, debido a que se encuentran localizados fuera de la zona de cobertura de los transmisores de sus contrapartes.

El ejemplo mostrado en la figura 14.8 muestra una LAN fragmentada. La ausencia de una conectividad completa de una red inalámbrica produce lo que se conoce como **problema de la terminal oculta**. Esto se presenta cuando dos nodos se encuentran localizados fuera

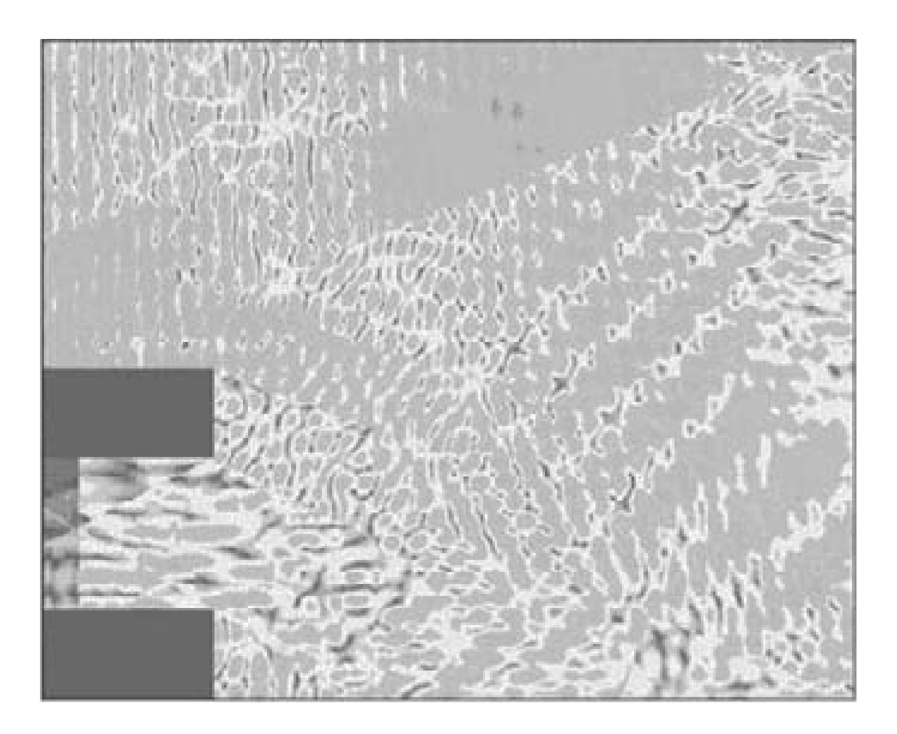


FIGURA 14.7 Distribución de la intensidad de una señal de radio.

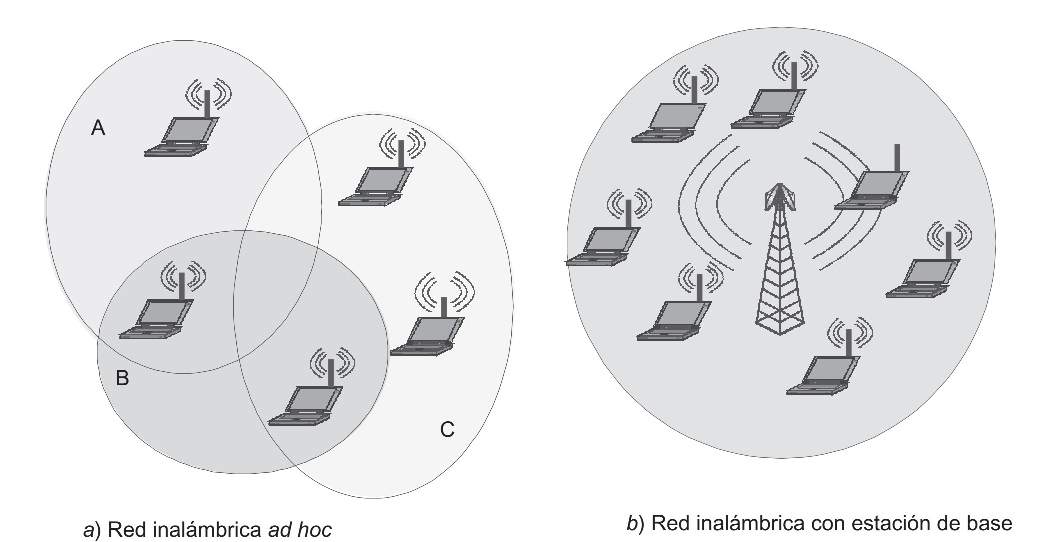


FIGURA 14.8 Conectividad de LAN inalámbrica.

de los límites de cada otro (los nodos A y C en la figura), pero un tercer nodo, B, es capaz de recibir las señales tanto de A como de C. Suponga que la red de radio utiliza un método de acceso tradicional basado en detección de la portadora, como CSMA/CD. En este caso, las colisiones serían mucho más frecuentes que en las redes tradicionales cableadas. Por ejemplo, supongamos que el nodo B intercambia información con el nodo A. El nodo C encontraba difícil detectar que el medio se encuentra ocupado y comenzará a transmitir su trama. Como resultado, las señales cerca del nodo B serían distorsionadas (es decir, se presentarán colisiones). En una LAN cableada, la probabilidad de tales colisiones sería mucho menor.

La **detección de colisiones** en una red de radio también es complicada, pues la señal del transmisor del nodo suprime la señal de un transmisor remoto. En consecuencia, es difícil, si no imposible, detectar la distorsión de la señal.

> Los métodos de acceso de las redes inalámbricas abandonan no sólo la detección de la portadora, sino también la detección de colisiones. En su lugar, ponen en marcha varios métodos de **prevención de colisiones (CA)**, incluido el **poleo**.

El uso de una **estación base** puede mejorar la conectividad de la red (figura 14.8*b*). La estación base por lo regular tiene mayor potencia y su antena en general está establecida para cubrir el territorio requerido de manera más fácil y uniforme. Como resultado, los nodos de una LAN inalámbrica son capaces de intercambiar información con la estación base, la cual sirve como un nodo de tránsito para el intercambio de información entre los nodos extremos de la red.

Las LAN inalámbricas resultan prometedoras para aplicaciones en las cuales es difícil o imposible usar LAN cableadas. Las principales áreas para la aplicación de la LAN inalámbrica son:

- *Acceso residencial* de proveedores alternos, los cuales no tienen acceso por cable a clientes que viven en edificios de departamentos.
- *Acceso móvil* en aeropuertos, estaciones de ferrocarril, etcétera.
- Organización de las LAN en edificios donde es imposible instalar un sistema de cableado moderno, como en edificios históricos con interiores originales.
- LAN temporales, necesarias para realizar una conferencia, por ejemplo: los conferenciantes que asisten a una sesión no pueden utilizar conexiones alámbricas.
- *Extensiones de la LAN*; por ejemplo, un edificio de una compañía (como un taller o laboratorio de pruebas) puede ser aislado de otros locales. Los pocos lugares de trabajo en un edificio de esta clase hacen ineficaz la instalación de cable. Por lo tanto, la comunicación inalámbrica demuestra ser más racional.
- *LAN móviles*. Si un usuario necesita tener acceso a la LAN mientras se desplaza de habitación en habitación o de un edificio a otro, las LAN inalámbricas no tienen competencia. Un doctor que visita a sus pacientes y usa una computadora portátil para conectarse a la base de datos del hospital es un ejemplo típico de un usuario de esta categoría.

Por el momento, las LAN móviles no pretenden cubrir completamente grandes territorios, como lo hacen las redes de teléfonos celulares móviles; sin embargo, tienen buen potencial para hacerlo. En el campo de las redes celulares móviles de edificios para la transmisión de datos, las tecnologías de LAN inalámbrica tendrán que competir con las **redes celulares móviles de tercera generación (3G)**. Las **redes celulares móviles de 2G** no son consideradas competidores serios, pues fueron diseñadas principalmente para transmisión de voz. Sus capacidades en el campo de la transmisión de datos están limitadas a velocidades de varios kilobits por segundo; las LAN inalámbricas aseguran velocidades de docenas de megabits por segundo. Sin embargo, se espera que las velocidades de transmisión en los sistemas 3G se encuentren entre los 144 Kps y los 2 Mbps (esta última velocidad se alcanzará a distancias pequeñas desde la estación base). De este modo, la competencia puede resultar bastante cerrada.

Más adelante en este capítulo se considerarán las LAN estándar inalámbricas más populares (IEEE 802.11). Aparte del IEEE 802.11 existen otros estándares en este campo: en

particular, el instituto de estándares europeo de telecomunicaciones (ETSI, por sus siglas para European Telecommunications Standards Institute) ha diseñado el estándar HIPER-LAN 1. Empero, la mayoría de los fabricantes produce equipo de acuerdo con las especificaciones IEEE 802.11.

14.4.2 Pila de protocolos IEEE 802.11

Naturalmente, la pila de protocolos de este estándar corresponde a la estructura común de los estándares del comité 802. Esto significa que consta de una capa física y una capa MAC sobre la cual funciona la capa LLC. Como todas las tecnologías de la familia 802, la **802.11** está definida por las dos capas inferiores: la capa física y la subcapa MAC. La subcapa LLC (LLC2) lleva a cabo sus funciones, las cuales son estándares para todas las tecnologías de LAN. Como las distorsiones de la trama son más probables en los medios inalámbricos que en los medios guiados, es más probable que LLC se utilice en el modo LLC2; sin embargo, esto no depende de la tecnología 802.11, pues el modo de operación LLC está seleccionado por los protocolos de capas superiores.

La estructura de la pila de protocolo IEEE 802.11 se muestra en la figura 14.9.

> En la *capa física* existen varias especificaciones que difieren en términos de intervalo de frecuencia, método de codificación y, en consecuencia, velocidades de información. Todas las variantes de la capa física trabajan con el mismo algoritmo de la capa MAC. No obstante, algunos parámetros de tiempo de la capa MAC dependen de la capa física que se utilice.

En 1997 el comité 802.11 adoptó el estándar y definió las funciones MAC con *tres variantes de la capa física* y aseguró velocidades de transmisión de datos de 1 y 2 Mbps.

- La primera variante utiliza **ondas infrarrojas** de 850 nm como medio de transmisión, las cuales son generadas mediante un diodo láser semiconductor o por medio de un diodo emisor de luz (LED, por sus siglas en inglés). Como las ondas infrarrojas no penetran las paredes, la cobertura de una LAN de esta clase se halla limitada por la línea de visión sin

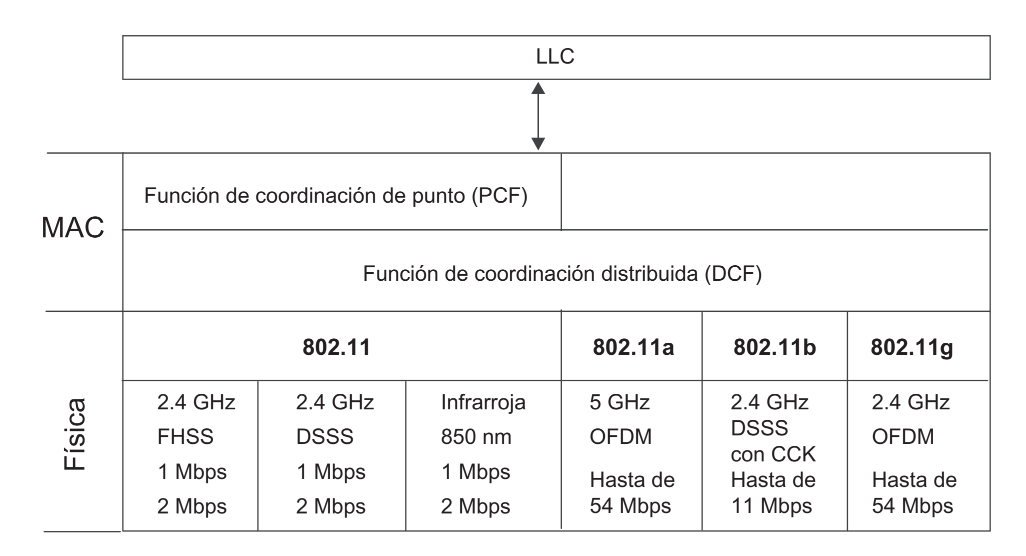


FIGURA 14.9 Pila de protocolo IEEE 802.11.

obstáculos. El estándar atiende las necesidades para las tres variantes de la propagación de onda: antenas omnidireccionales, reflejo desde el techo y radiación direccional enfocada. En el primer caso, un haz estrecho se difunde utilizando un sistema de lentes. La última variante está destinada para organizar las comunicaciones "punto a punto" entre, por ejemplo, dos edificios.

- La segunda variante emplea el **intervalo de microondas** de 2.4 GHz, el cual, basado en las recomendaciones de la ITU, no tiene licencia en la mayoría de los países. Una variante de microondas de la capa física usa FHSS, mientras que la otra emplea DSSS.[1] Cuando se utiliza FHSS, cada canal tiene una anchura de 1 MHz. Al usar modulación FSK, dos estados (frecuencias) de señal proporcionan una tasa o velocidad de 1 Mbps y al emplear cuatro estados de señal se produce una tasa de 2 Mbps. Cuando se utiliza FHSS, la red puede constar de células; para eliminar la interferencia mutua, las células vecinas pueden usar secuencias de frecuencia ortogonales. El número de canales y la frecuencia de conmutación entre los canales son parámetros configurables, de manera que los instaladores de la LAN inalámbrica pueden tener en cuenta características específicas de regulación del espectro de frecuencias para un país en especial. Por ejemplo, en Estados Unidos pueden utilizarse hasta 79 canales dentro de un canal de 2.4 GHz de ancho, y el máximo tiempo que se pasa en cada canal no debe exceder los 400 milisegundos.
- La tercera variante, que también emplea el mismo *intervalo de microondas* de 2.4 GHz, está basada en la *codificación DSSS*. Ésta utiliza el código de 11 bits 10110111000 como una secuencia granular. Cada byte es codificado empleando BPSK (1 Mbps) o QPSK (2 Mbps).

En 1999 se aprobaron otras dos variantes de la capa física: **802.11a** y **802.11b**.

- La especificación consigue la velocidad o tasa de información incrementada al usar un intervalo de frecuencias superior: 5 GHz. Para este propósito, dicha tecnología emplea 300 MHz de tal intervalo, multiplexado de división de frecuencia ortogonal (OFDM, por sus siglas para Orthogonal Frequency Division Multiplexing) y FEC. Las tasas de información que se consiguen incluyen 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. El intervalo de 5 GHz, empleado por el 802.11a, actualmente se encuentra muy poco poblado y asegura altas tasas de información. No obstante, el uso de éste intervalo provoca dos problemas: el primero, que el equipo para funcionar a estas frecuencias todavía es bastante costoso; y el segundo, que en algunos países este intervalo se encuentra asignado.
- La segunda especificación, *IEEE 802.11b*, aún emplea 2.4 GHz, lo que permite el uso de equipo más económico. Para aumentar la velocidad hasta los 11 Mbps, la cual es comparable con la del Ethernet clásico, esta tecnología utiliza el método DSSS más eficiente y usa la **manipulación por código complementario** (CCK), un esquema de modulación mejorado que fue adoptado en 1999 para reemplazar el **código Barker** en las redes digitales inalámbricas (véase el capítulo 10).

Uno de los últimos estándares del grupo 802.11 para la capa física, el **802.11g**, fue probado en el verano de 2003.

- El *IEEE 802.11g* también funciona a 2.4 GHz, pero asegura velocidades de transmisión de datos hasta de 54 Mbps. Esta especificación también usa OFDM. Hasta hace poco, las reglas en Estados Unidos permitían aplicar solamente una técnica del espectro extendido a 2.4 GHz. La eliminación de esta limitación ofreció incentivos para nuevas investigaciones e

[1] Se ofrece información más detallada de estos métodos en el capítulo 10.

innovaciones, como resultado de las cuales han aparecido nuevas tecnologías inalámbricas de alta velocidad. Para proporcionar la compatibilidad hacia atrás con 802.11b, también se soporta CCK.

El diámetro de una red 802.11 depende de muchos parámetros, incluido el intervalo de frecuencia utilizado. Normalmente, el diámetro de una LAN inalámbrica se encuentra entre los 100 y los 300 m.

La capa MAC realiza más funciones en las LAN inalámbricas que en las redes cableadas. Las funciones MAC en el estándar 802.11 incluyen las siguientes:

- Proporcionar acceso al medio compartido.
- Asegurar la movilidad de la estación cuando estén disponibles varias estaciones base.
- Asegurar la misma seguridad que la de las LAN cableadas.

14.4.3 Topologías de las LAN 802.11

El estándar 802.11 soporta dos tipos de topologías LAN: redes *ad hoc*, también conocidas como *conjunto de servicios básicos* (BSS) y redes con infraestructura, denominadas *conjunto de servicios extendidos* (ESS).

Las *redes ad hoc*, que de acuerdo con la terminología 802.11 se les denomina **conjunto de servicios básicos (BSS)**, son creadas mediante *estaciones individuales.* No contienen una estación base y los nodos en tales redes se comunican directamente entre sí (figura 14.10). Para convertirse en miembro de un BSS, la estación debe realizar el procedimiento de asociación.

Los BSS no son células tradicionales en términos de zonas de cobertura porque pueden localizarse muy apartadas. También pueden traslaparse de modo parcial o por completo. El estándar 802.11 proporciona en este aspecto la libertad para la arquitectura de la red.

En las redes con infraestructura, algunas estaciones son estaciones base. En la terminología 802.11, las estaciones base se denominan **puntos de acceso (AP)**. Una estación que

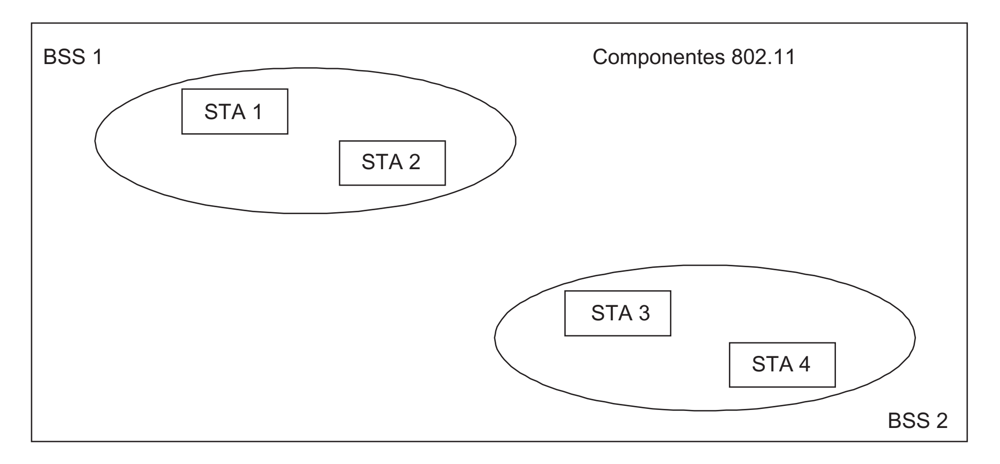


FIGURA 14.10 Conjunto de servicios básicos.

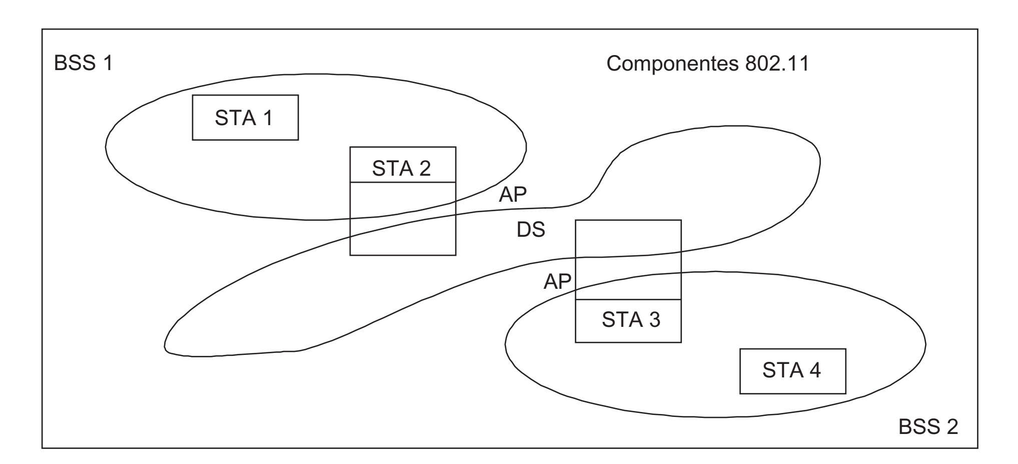


FIGURA 14.11 Conjunto de servicios extendido y sistema de distribución.

realiza funciones de AP es un miembro de un BSS (figura 14.11). Todos los AP de la red están conectados entre sí mediante el *sistema de distribución* (DS, por sus siglas en inglés). El papel que desempeña el DS puede establecerse por el medio utilizado para interconectar estaciones (por ejemplo, ondas de radio o infrarrojas) o con un medio diferente, como el cableado. Con el DS, los AP llevan a cabo el **servicio del sistema de distribución (DSS)**. La tarea del DSS consiste en transmitir paquetes entre estaciones que por alguna razón no pueden (o no quieren) interactuar en forma directa. La razón más evidente para usar DSS es si las estaciones pertenecen a distintos BSS. En este caso, transmiten las tramas a sus AP, los cuales utilizan el DS para transmitir aquellas tramas al AP que sirven al BSS al que pertenece la estación de destino.

Las redes del **conjunto de servicios extendidos (ESS)** son aquellas que constan de varios BSS conectados por un DS en un ESS en la terminología 802.11.

Los ESS aseguran movilidad para las estaciones, porque pueden moverse de un BSS a otro. Estos movimientos están asegurados por las funciones de la capa MAC de ambas estaciones y APS; por lo tanto, son transparentes para la capa LLC. Un ESS también puede comunicarse con una LAN cableada. Para este propósito, el DS debe contener un **portal**.[2]

14.4.4 Acceso al medio compartido

Las estaciones pueden emplear el medio compartido para los propósitos siguientes:

- Transmitir datos de manera directa entre sí dentro de una BSS simple.
- Transmitir datos dentro de una BSS simple usando un AP como nodo de tránsito.
- Transmitir datos entre BSS utilizando dos AP y el DS.
- Transmitir datos entre una BSS y una LAN cableada empleando un AP, un DS y un portal.

[2] Las funciones de un portal no están definidas con detalle: esta función puede realizarla un conmutador o un enrutador.

En redes 802.11, la capa MAC asegura dos modos para el acceso al medio compartido:

- **Función de coordinación distribuida (DCF).**
- **Función de coordinación de un punto (PCF).**

Modo de acceso de la función de coordinación distribuida

En primer lugar, considere el método para proporcionar acceso utilizando DCF. Este método implementa el conocido algoritmo CSMA/CD, el cual pertenece a la clase de algoritmos CA basados en la detección o sensado de la portadora. Al mismo tiempo, utiliza un "algoritmo ranurado". En lugar de un procedimiento directo para detectar colisiones basado en el estado del medio, el cual es ineficaz en redes inalámbricas, este método utiliza detecciones de colisión indirecta. Para este propósito, cada trama transmitida debe ser confirmada por una trama ACK enviada por la estación de destino. Si no se recibe un ACK durante el tiempo de interrupción predeterminado, el remitente considerará que ha ocurrido una colisión.

El uso de un algoritmo de acceso ranurado requiere que las estaciones estén sincronizadas. En las tecnologías 802.11, este problema tiene una solución elegante: el conteo de los espacios de tiempo comienza cuando se consume la transmisión de la siguiente trama (figura 14.12). Esto no requiere transmitir señales especiales de sincronización, ni limita el tamaño del paquete por el tamaño de la ranura, debido a que las ranuras se tienen en cuenta sólo cuando se toma una decisión al iniciar la transmisión de la trama.

Una estación que necesita transmitir una trama primero debe detectar la portadora. Cuando registra el final de la transmisión de la trama, debe esperar el espacio de tiempo del *espacio entre tramas* (IFS, InterFrame Space). Si después de transcurrir el IFS, el medio todavía está libre, iniciará el conteo de ranuras, cada una de las cuales tiene la duración *SlotTime*. Es posible comenzar la transmisión de la trama solamente cuando comienza una ranura, a condición de que el medio se encuentre libre. La estación elige la ranura con base en el **algoritmo exponencial binario truncado de retirada**, semejante al utilizado en CSMA/CD. El número de ranuras se elige como un entero aleatorio, equitativamente distribuido dentro del intervalo [0, CW], donde CW quiere decir **ventana de contención (Contention Window)**.

El método de selección del tamaño de ranura y el tamaño de la ventana de contención se verá más adelante en este capítulo. Por el momento, considere este complicado método de acceso con un ejemplo práctico (figura 14.12). Supongamos que la estación A ha elegido la ranura 3 para transmitir con base en el algoritmo exponencial binario truncado de retirada. Una vez seleccionado el número de ranura, la estación asigna el valor 3 al **temporizador de**

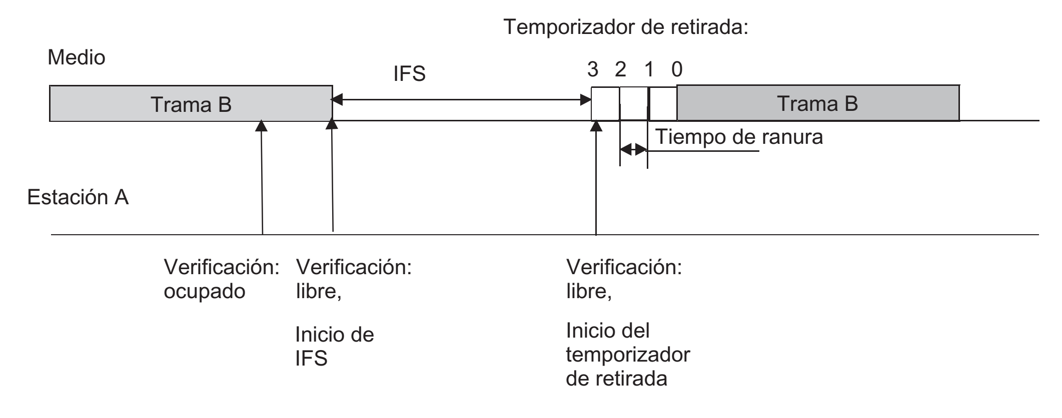


FIGURA 14.12 Algoritmo DCF.

retirada (cuyo propósito se aclarará a partir de la discusión adicional) y comienza a verificar el estado del medio al principio de cada ranura. Si el medio se encuentra disponible, el valor del temporizador de retirada disminuirá en 1. La transmisión de la trama comenzará si el resultado es 0.

> De este modo, el algoritmo asegura que todas las ranuras, incluida la actual, se encuentran disponibles. Esta condición es esencial y debe observarse para el comienzo de la transmisión**.**

Si el medio se encuentra ocupado al principio de una ranura específica, el contador se "congelará" (es decir, no disminuirá en 1). Si esto pasa, la estación empezará un nuevo ciclo para el acceso al medio, cambiando sólo el algoritmo utilizado para seleccionar la ranura para la transmisión. Como en el ciclo anterior, la estación continúa la detección de la portadora. Cuando el medio está libre de nuevo, la estación hace una pausa, cuya duración es igual al IFS. Si el medio continúa libre después de este intervalo, la estación utilizará el valor congelado del temporizador de retirada como el número de ranura, y realizará el procedimiento descrito con anterioridad para verificar ranuras libres y disminuir el temporizador de retirada a partir de su valor congelado.

El *tamaño de la ranura* depende del método de codificación de la señal, pues para el método FHSS el tamaño de la ranura es de 28 µseg, mientras que para el método DSSS es de 1 µseg. El tamaño de la ranura se elige para exceder el valor del tiempo de propagación de la señal entre cualesquiera dos estaciones, más el tiempo requerido para que la estación reconozca de manera correcta la disponibilidad del medio. Si este requerimiento es satisfecho, cada estación podrá reconocer correctamente el inicio de la transmisión de la trama cuando detecta las ranuras precedentes a la que sea seleccionado para transmisión. Esto a su vez significa lo siguiente:

> Puede ocurrir una colisión solamente cuando se eligen varias estaciones en la misma ranura para transmisión.

Si ocurre una colisión, las tramas se distorsionarán y ninguna trama de ACK llegará desde las estaciones de destino. Si las estaciones no reciben un ACK desde la estación de destino durante un periodo predeterminado, registrarán una colisión e intentarán volver a transmitir sus tramas. Después de cada intento fallido de transmisión de la trama, el intervalo [0, CW] del cual se seleccionaron los números de ranura es duplicado. Por ejemplo, si el tamaño de ventana inicial fue seleccionado para ser igual a 8 (es decir, CW = 7), la ventana deberá establecerse a 16 (CW = 15) después de la primera colisión. Luego de la segunda colisión, el tamaño de ventana debe ser establecido a 32, y así sucesivamente. El estándar 802.11 específica que el valor inicial de la CW debe seleccionarse según el tipo de la capa física utilizado en la LAN inalámbrica.

Como en CSMA/CD, el número de intentos fallidos de retransmisión de una trama está limitado; sin embargo, el estándar 802.11 no proporciona un valor exacto para este límite superior. Cuando el límite superior de *N* intentos fallidos se alcanza, se descarta la trama y el número de colisiones se establece en 0. Naturalmente, si después de un número de intentos fallidos la estación consigue enviar una trama de manera exitosa, el contador también se establece en 0.

DCF toma medidas especiales para eliminar el **efecto de terminal oculta**. Para este propósito, la estación que necesita capturar el medio y, de acuerdo con el algoritmo descrito, decide

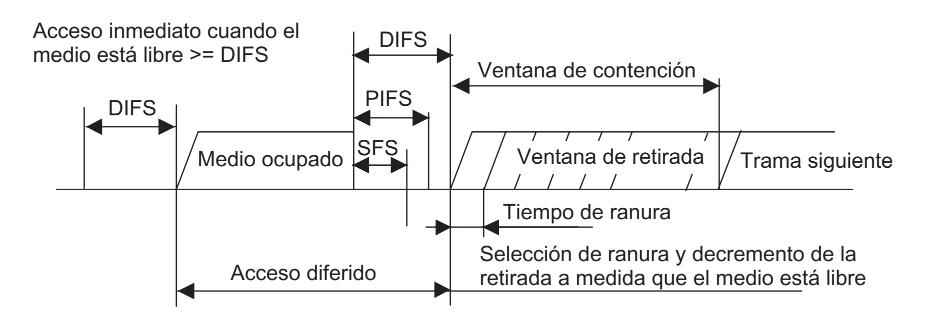


FIGURA 14.13 Coexistencia de PCF y DCF.

comenzar la transmisión de la trama en una ranura específica debe enviar una breve *trama de solicitud de envío* (*RTS, Request-To-Send*) en lugar de la trama de datos hacia la estación de destino. La estación de destino debe responder con una *trama lista para enviar* (*CTS, Clear-To-Send*), después de lo cual la estación fuente envía la trama de datos. La trama CTS debe contener información acerca de la captura del medio destinada a todas las estaciones fuera del alcance de la estación de envío pero dentro de la zona de cobertura de la estación de destino (es decir, hacia las estaciones que son terminales ocultas para el remitente).

NOTA *La longitud máxima de la trama de acuerdo con el estándar 802.11 es de 2 346 bytes, la longitud de RTS es de 20 bytes y la trama CTS toma 14 bytes. Puesto que las tramas RTS y CTS son considerablemente más cortas que la trama de datos, las pérdidas causadas por las colisiones de las tramas RTS o CTS son bastante más pequeñas que las pérdidas originadas por las colisiones de las tramas de datos. El procedimiento de intercambio de las tramas RTS-CTS es opcional: puede abandonarse cuando la carga de la red es baja, pues en este caso las colisiones son raras, lo cual significa que no hay necesidad de gastar tiempo adicional llevando a cabo el procedimiento RTS-CTS.*

Modo de acceso de la función de coordinación de un punto

Si el BSS contiene una estación que realiza funciones de AP, podrá emplearse el método de acceso centralizado implementado por el algoritmo PCF. Este método asegura la prioridad al servicio del tráfico. En tal caso, el AP lleva a cabo las funciones de **coordinador de punto** (PC)[3] (por ejemplo, árbitro del medio).

En las redes 802.11, PCF coexiste con DCF. Su cooperación está coordinada utilizando tres tipos de IFS (figura 14.13).

Después de que el medio es liberado, cada estación cuenta el tiempo libre del medio, comparado con los valores de tres intervalos:

- IFS corto (**SIFS, Short IFS**).
- PCF IFS (**PIFS**).
- DCF IFS (**DIFS**).

El procedimiento de captura del medio utilizando el algoritmo DCF descrito es posible sólo cuando el medio está libre por un tiempo mayor o igual al de DIFS. Esto significa que

[3] En esta sección, PC significa coordinador de punto.

cuando se describe la operación del algoritmo DCF, DIFS (es decir, el más extenso de los tres intervalos posibles) debe ser utilizado como IFS. Esto da al método DCF la prioridad más baja.

El valor más pequeño, SIFS, está destinado a capturar el medio de más alta prioridad mediante tramas CTS o ACK, que continúan o consiguen la transmisión de trama que ha comenzado.

PIFS es más extenso que SIFS, pero más pequeño que DIFS. El intervalo igual a la diferencia entre DIFS y PIFS es utilizado como el árbitro del medio (es decir, el PC). Durante este intervalo, puede transmitir una trama especial de faro, mas no las estaciones que ha comenzado el **periodo libre de contención**. Una vez recibida una trama de faro, las estaciones que quisieran utilizar el algoritmo DCF para capturar el medio ya no pueden hacerlo. Para capturar el medio, deben esperar hasta que transcurra el periodo libre de contención. La duración de este periodo está declarada en la trama de faro, aunque puede transcurrir más rápido si las estaciones no tienen tráfico sensible al retardo. En este caso, el PC transmite la trama de final de CF (CF-End), después de la cual el método de acceso DCF comienza a funcionar, a condición de que haya transcurrido el DIFS.

Durante el intervalo libre de contención, el PC utiliza el procedimiento de poleo para permitir a cada estación que participa en PCF transmitir su trama. Para lograr esto, el PC en turno envía una trama especial CF-POLL a cada estación participante, dándole así la oportunidad de usar el medio. Una vez recibida esta trama, la estación puede responder con la trama CF − ACK + DATA, que confirma la recepción de la trama CF-POLL y transmite datos de manera simultánea (ya sea a la dirección PC para transmisión de tránsito o directamente a la estación de destino).

Para asegurar que el tráfico asincrónico siempre obtenga alguna parte del ancho de banda, la duración del periodo libre de contención está limitada. Cuando transcurre este periodo, el PC transmite la trama CF-End y comienza el período de contención.

Cualquier estación puede participar en PCF. Para este propósito, tiene que suscribirse a este servicio cuando se conecta a la red (es decir, cuando lleva a cabo el procedimiento de asociación).

14.4.5 Seguridad

Los diseñadores del IEEE 802.11 establecieron el objetivo de asegurar la seguridad de la transmisión de datos al usar una LAN inalámbrica de manera equivalente a la seguridad de la transmisión de datos usando una LAN cableada, como Ethernet.

La descripción de Ethernet cableado no incluía medidas especiales dirigidas a garantizar la seguridad de los datos. Los estándares de Ethernet no implementan la autenticación del usuario o la encriptación de los datos. Sin embargo, las redes cableadas están mejor protegidas en contra de accesos no autorizados o violaciones de la confidencialidad que las LAN inalámbricas, debido simplemente a que están cableadas: el intruso debe conectarse de manera física a una red cableada para tener acceso a ella. Para este propósito, el intruso debe penetrar de alguna manera a locales equipados con enchufes y conectar la computadora atacante a uno de ellos. Está acción puede ser advertida y prevenida, aunque todavía es posible obtener acceso no autorizado a una LAN cableada.

En una LAN inalámbrica, es mucho más fácil conseguir un acceso no autorizado. Es suficiente estar dentro del alcance de una LAN de esta clase. Para penetrar con éxito una LAN inalámbrica, no es necesario entrar a las instalaciones donde funciona esa LAN, ni una conexión física al medio, porque el visitante puede recibir datos sin levantar ninguna sospecha. Simplemente basta con tener una computadora portátil encendida en una bolsa.

El estándar 802.11 proporciona herramientas de seguridad que elevan el nivel de seguridad de una LAN inalámbrica al de una LAN normal cableada. Por lo tanto, el principal protocolo de seguridad de datos en la red 802.11 se denomina **privacidad equivalente alámbrica (WEP)**, la cual permite encriptar los datos transmitidos al usar un medio inalámbrico, asegurando así la confidencialidad. Otro mecanismo de seguridad en las redes inalámbricas es un mecanismo de autenticación: *la verificación del sujeto original que permite que únicamente los usuarios autorizados se conecten.* Sin embargo, las herramientas de seguridad de las redes 802.11 son un blanco popular de las críticas debido a que no proporcionan una protección confiable de los datos como las herramientas de seguridad similares de otros estándares. Por ejemplo, mediante el rastreo del tráfico encriptado 802.11, un intruso especializado puede descifrar la información en 24 horas. Por lo tanto, el grupo de trabajo 802.11i desarrolla un estándar más eficaz para proteger los datos en las redes 802.11.

14.5 PAN Y BLUETOOTH

PALABRAS CLAVE: PAN (Personal Area Networks, redes de área personal), grupo de interés especial en Bluetooth (Bluetooth SIG, Special Interest Group), maestro, esclavos, piconet, medio compartido piconet, scatternet, enlace sincrónico orientado a la conexión (SCO, Synchronous Connection-Oriented), enlace asincrónico sin conexión (ACL, Asynchronous ConnectionLess), FHSS y modulación BFSK.

14.5.1 Características específicas de las PAN

Las **PAN (Personal Area Networks o redes de área personal)** están destinadas para comunicaciones entre dispositivos pertenecientes a un solo propietario a través de distancias pequeñas, por lo regular de 10 metros. Ejemplos de dispositivos de esta clase son computadoras portátiles (notebooks), teléfonos móviles, impresoras, asistentes digitales personales (PDA), equipos de televisión y numerosos aparatos domésticos de alta tecnología, como refrigeradores.

Las PAN deben proporcionar acceso fijo (por ejemplo, dentro de un hogar) o móvil (por ejemplo, cuando el propietario se mueve entre habitaciones, edificios o ciudades llevando los dispositivos).

Las PAN son semejantes a las LAN en muchos aspectos, pero también tienen características específicas.

- Muchos dispositivos destinados a participar en una PAN son *mucho más simples* que las computadoras, que son los típicos nodos de una LAN; además, tales dispositivos suelen ser pequeños y económicos. Por lo tanto, los estándares de las PAN deben tener en cuenta que la implementación de la PAN debe producir soluciones económicas con un bajo consumo de energía.
- *Un área de cobertura PAN es más pequeña que la de una LAN.* Para la interacción entre nodos de PAN, por lo general es suficiente una distancia de varios metros.
- *Requerimientos estrictos para la seguridad.* Los dispositivos personales que transporta el propietario a menudo deben trabajar en diferentes entornos. En ocasiones necesitan comunicarse con dispositivos de otras PAN, como cuando un usuario se encuentra con un colega o amigo en alguna parte y deciden intercambiar direcciones almacenadas en las libretas de direcciones de sus PDA. En otros casos, tal interacción es en extremo

indeseable, porque puede producir la filtración de información confidencial. Debido a esto, los protocolos PAN deben asegurar varios métodos de autenticación del dispositivo y encriptación de datos en el entorno móvil.

- Cuando se interconectan pequeños dispositivos móviles, la necesidad de deshacerse de los cables es más evidente que, digamos, cuando se conecta una impresora a una computadora o concentrador. Debido a esto, *las PAN tienden a favorecer las soluciones inalámbricas más de lo que lo hacen las LAN.*
- Si el usuario transporta de manera constante el dispositivo PAN, no deberá causar daño a la salud de los usuarios. Por lo tanto, las señales emitidas por un dispositivo de esta clase deben ser de *baja potencia*, de preferencia que no excedan los 100 mW. (Un teléfono celular normal emite señales en el intervalo de los 600 mW a los 3 W.)

En la actualidad, la tecnología PAN más popular es Bluetooth, la cual asegura la interacción de hasta ocho dispositivos utilizando un medio compartido a 2.4 MHz y a velocidades de hasta 723 Kbps.

14.5.2 Arquitectura Bluetooth

El estándar Bluetooth fue diseñado por el **Grupo de Interés Especial en Bluetooth (Bluetooth SIG, Special Interest Group)** organizado por iniciativa de Ericsson. El estándar Bluetooth también ha sido adoptado por el grupo de trabajo IEEE 802.15.1 a través de la estructura común de los estándares IEEE 802.

La tecnología Bluetooth utiliza el concepto de **piconet**. El nombre de este concepto destaca la pequeña área de cobertura de tales redes, de 10 a 100 metros, según la potencia del dispositivo transmisor Bluetooth.

Una piconet puede reunir hasta 255 dispositivos. No obstante, solamente ocho de estos dispositivos pueden estar activos y llevar a cabo intercambio de datos en cualquier momento. Uno de los dispositivos piconet es el **maestro**; los otros dispositivos son **esclavos** (figura 14.14). El maestro es responsable de proporcionar acceso al medio compartido de la piconet, que representa frecuencias no asignadas de la gama de 2.4 GHz. Tal arquitectura permite utilizar protocolos más simples en dispositivos esclavos (como audífonos para radio) y funciones de administración de red más complejos para delegarse a la computadora y lo más probable con el fin de convertirse en un dispositivo maestro para una red de esta clase.

De esa forma, cada piconet tiene un maestro y hasta siete esclavos activos. Un esclavo activo puede intercambiar datos solamente con su maestro. El intercambio directo de datos entre esclavos es imposible. Todos los dispositivos esclavos de la piconet actual, con excepción de los siete activos, deben funcionar en modo PARK, caracterizado por un bajo consumo de energía. Cuando se funciona de este modo, los esclavos escuchan periódicamente los comandos (órdenes) del maestro para conmutarse al estado activo.

El maestro es el responsable de tener acceso al **medio compartido de la piconet**, que representa frecuencias no asignadas (licenciadas) de la gama de 2.4 GHz. El medio compartido transmite datos a 1 Mbps, aunque, debido al encabezado del paquete y al gasto general con salto de frecuencias, la tasa o velocidad efectiva de información del medio no excede 777 Kbps. El maestro divide el ancho de banda medio entre siete dispositivos esclavos con fundamento en la técnica de multiplexado por división del tiempo (TDM).

Tal arquitectura permite usar protocolos más simples en dispositivos esclavos (por ejemplo, auriculares) y delega las funciones más complicadas de la administración de la red a una computadora que, muy probablemente, se convierte en el maestro de la piconet.

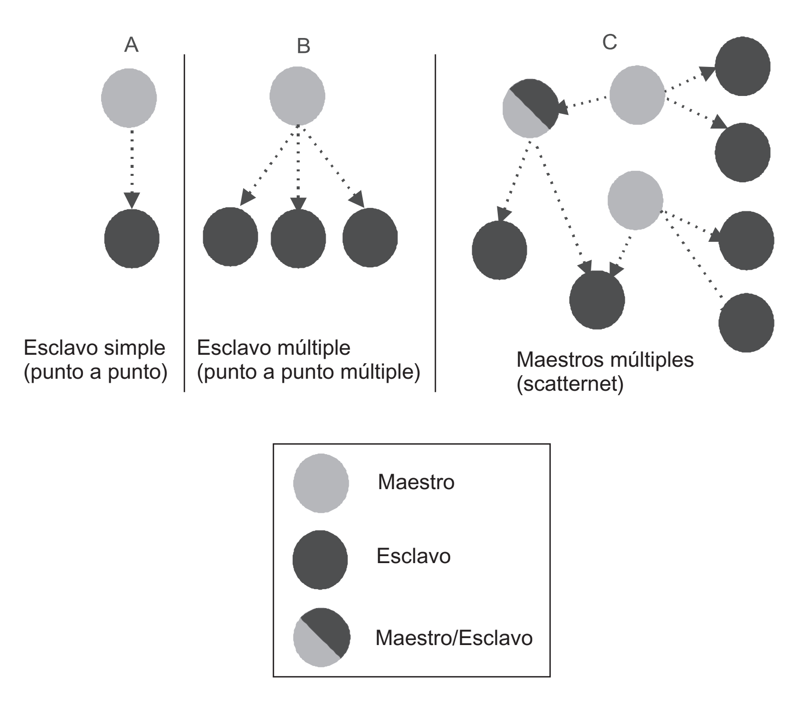


FIGURA 14.14 Piconet y scatternet.

El procedimiento para conectar una piconet es dinámico. El maestro de la piconet recolecta periódicamente información en los dispositivos que se hallan dentro de la zona de su piconet mediante el poleo (sondeo) de éstos. Dicho procedimiento se conoce como *búsqueda*. Después de detectar un nuevo dispositivo, el maestro lleva a cabo el procedimiento de negociación con ese dispositivo. Si la intención del dispositivo esclavo para conectarse a la piconet coincide con la del maestro (lo cual significa que el dispositivo ha realizado el procedimiento de autenticación y pertenece a la lista de dispositivos permitidos), el maestro conecta el nuevo dispositivo a su red.

NOTA *La seguridad en las redes Bluetooth está asegurada por la autenticación de dispositivos y la encriptación del tráfico. Los protocolos Bluetooth aseguran un mayor nivel de protección que el protocolo WEP del estándar IEEE 802.11.*

Varias piconets que se hallan dentro de la misma zona y llevan a cabo intercambio de datos forman una **scatternet**; a su vez, las piconets que forman una scatternet pueden interactuar, debido a que el mismo nodo puede ser parte de manera simultánea de varias piconets. Un dispositivo de esta clase por lo general se denomina *puente*. La diferencia entre la scatternet y la ESS 802.11 estándar es que en la scatternet no hay analogías con la AP a través de la cual interactúan redes separadas (más precisamente BSS). En la scatternet, el mismo nodo puede desempeñar el papel de maestro en una piconet y el papel de esclavo en otra.

Para evitar la interferencia de las señales de diferentes piconets, cada maestro utiliza su *propia* secuencia de saltos. Usar diferentes secuencias de saltos complica el proceso de la interoperación de la piconet. Para conseguir la interoperación, el dispositivo que desempeña el papel de un puente debe, a su vez, ser parte de cada piconet que cambia su secuencia de frecuencia.

Aunque las colisiones son poco probables, todavía pueden tener lugar cuando los dispositivos de diferentes piconets eligen el mismo canal de frecuencia para su operación. Sin embargo, la probabilidad de esto es pequeña, pues es posible que el número de piconets en la misma área sea pequeño.

De acuerdo con la descripción del estándar, una scatternet implementa CDMA con base en FHSS.

Para asegurar la transmisión confiable de los datos, Bluetooth utiliza FEC. Cuando se transmiten los datos, la recepción de la trama es confirmada mediante el empleo de acuses de recibo. La codificación FEC no es un método obligatorio.

Las redes Bluetooth utilizan diferentes métodos para transmitir información de las siguientes clases:

- Para tráfico sensible al retardo, la red soporta **enlaces sincrónicos orientados a la conexión (SCO)**. Para el canal SCO, el ancho de banda está reservado para todo el tiempo de conexión; por su parte, los canales SCO normalmente se utilizan para transmitir tráfico de voz a 64 Kbps.
- Para el tráfico elástico existe el **enlace asincrónico sin conexión (ACL)**. Para el canal ACL, el ancho de banda es asignado mediante una solicitud desde un esclavo o de acuerdo con las necesidades del maestro. Los canales ACL están destinados al tráfico de computadora a velocidades variables.

14.5.3 Pila de protocolos Bluetooth

Bluetooth es una tecnología original y funcionalmente completa destinada al uso autónomo en dispositivos electrónicos personales. Por esta razón, soporta una pila de protocolos completa, que incluye sus protocolos de aplicación. Ésta es su principal diferencia con las tecnologías consideradas con anterioridad, como Ethernet o IEEE 802.11, las cuales sólo llevan a cabo las funciones de la capa física y de la capa de enlace de datos.

La introducción de protocolos de aplicación internos, interconstruidos en Bluetooth, se explica por el deseo de sus diseñadores para implementar la tecnología en diversos dispositivos simples que no pueden soportar (y en la práctica, no necesitan hacerlo) la pila TCP/IP.

Bluetooth apareció como resultado de los intentos para desarrollar un estándar para la interacción entre un teléfono móvil y audífonos inalámbricos. Evidentemente, no tiene sentido utilizar complicados protocolos (como FTP o HTTP) para resolver esta tarea.

En consecuencia, se diseñó un complicado juego de protocolos, además del cual aparecieron considerables perfiles.

Los **perfiles** definen el conjunto específico de protocolos requerido para llevar a cabo una tarea en especial. Por ejemplo, existe un perfil para la interacción entre una computadora o teléfono móvil y auriculares inalámbricos (el perfil Headset o Auriculares). También hay un perfil de transferencia de archivos dirigido a dispositivos que pueden transferir archivos (los auriculares probablemente no lo utilizarán, aunque es difícil predecir el futuro) y un perfil para emulación del puerto RS-232.

Cuando se introdujeron los estándares Bluetooth en línea con la arquitectura del estándar IEEE 802, el grupo de trabajo IEEE 802.15.1 se limitó a los *protocolos del núcleo Bluetooth*, que corresponden a las funciones de las capas física y MAC (figura 14.15).

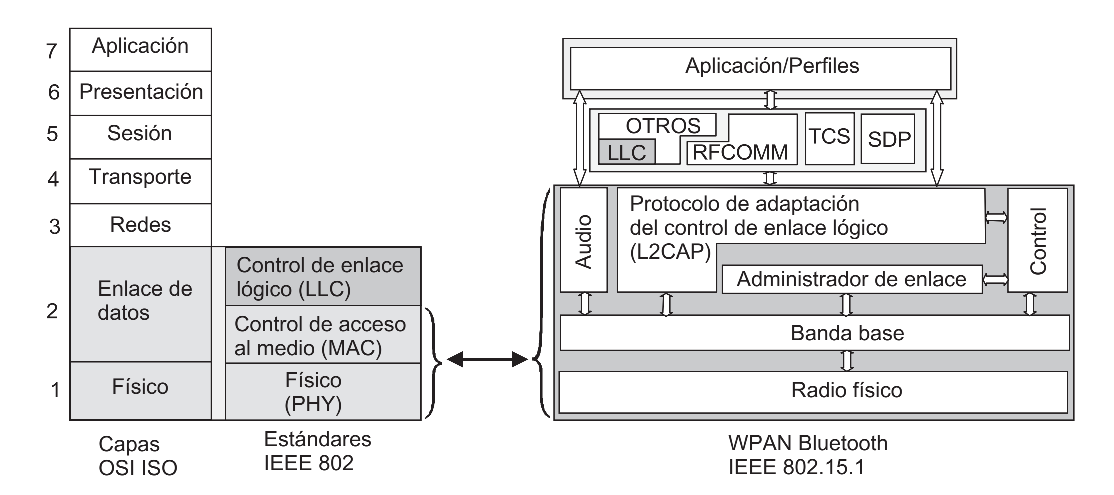


FIGURA 14.15 Correspondencia de los estándares del protocolo Bluetooth, el modelo OSI y el IEEE 802.

- La capa de *radio física* describe frecuencias y potencias de señales utilizadas para transmitir la información.

- La capa de *banda base* es responsable de la organización de enlaces en el medio radial. Estas responsabilidades de la capa incluyen la selección de la secuencia de saltos, de la sincronización de los dispositivos de la piconet y de la formación y transmisión de las tramas a través de los enlaces establecidos SCO y ACL. La trama Bluetooth tiene una longitud variable: su campo de datos puede constituirse desde 0 hasta 2 744 bits (343 bytes). Para transmisión de voz se utilizan tramas de longitud fija con campos de datos de 240 bits (30 bytes).

- El *administrador de enlace* es responsable de la autenticación del dispositivo y de la encriptación del tráfico. Aparte de esto, controla el estado del dispositivo, tal como el cambio de esclavo a maestro.

- La *capa de adaptación de control de enlace lógico* (L2CAP) es la capa superior de los protocolos centrales de Bluetooth. Este protocolo es utilizado únicamente cuando el dispositivo transmite datos. El tráfico de voz desvía este protocolo y se dirige directamente a la capa de banda base; a su vez, la capa L2CAP recibe segmentos de datos de 64 KB desde las capas superiores y los divide en tramas pequeñas para la capa de banda base. Cuando recibe las tramas, la capa L2CAP ensambla las tramas en un segmento inicial y transfiere éste hacia el protocolo de la capa superior.

- La *capa de audio* asegura la transmisión de voz a través de canales SCO. Esta capa aplica modulación por codificación de pulsos (PCM), lo cual define una velocidad del canal de voz de 64 Kbps.

- La *capa de control* transmite toda la información acerca del estado de la conexión hacia la unidad externa y recibe comandos u órdenes que modifican el estado y la configuración del dispositivo desde las unidades externas.

14.5.4 Tramas Bluetooth

El medio compartido es una secuencia de canales de frecuencia FHSS en la gama de los 2.4 GHz. Cada canal tiene 1 MHz de ancho. El número de canales es 79 (en Estados Unidos, la mayor parte de Europa y la mayoría de otros países) o 23 (en España, Francia y Japón).

La velocidad granular es de 1 600 Hz, de manera que el periodo de granulación es de 625 µseg. El maestro divide el medio compartido según indica la técnica TDM, utilizando el tiempo que requiere el sistema para cada canal de frecuencia (por ejemplo, 625 µseg) como una ranura de tiempo. La información es codificada a la frecuencia de reloj de 1 MHz al usar modulación BFSK. Como resultado, la velocidad de bit es de 1 Mbps.

Durante una sola ranura de tiempo, la piconet Bluetooth transmite 625 bits; sin embargo, no todos ellos son utilizados para transmitir información del usuario. Cuando se salta a otra frecuencia, los dispositivos de la red necesitan algún tiempo para sincronización, de manera que solamente 366 de los 625 bits son empleados para transmitir tramas de información.

Una trama de información puede tomar una, tres o cinco ranuras. Cuando la trama toma más de una ranura, la frecuencia del canal permanece sin cambios durante todo el tiempo de la transmisión de la trama. En tal caso, el gasto general para la sincronización es más pequeño. De esta manera, el tamaño de una trama que consta de cinco ranuras secuenciales es de 2 870 bits (el tamaño del campo de datos puede tomar hasta 2 744 bits).

NOTA *Únicamente las tramas de datos (por ejemplo, tramas del canal ACL) pueden constar de varias ranuras; las tramas que transmiten datos de voz (por ejemplo, tramas del canal SCO) siempre constan de sólo una ranura.*

Considere el formato de una trama que comprende una sola ranura: 366 bits (figura 14.16).

De los 366 bits que conforman la trama:

- 240 son asignados al *campo de datos.*
- 72 son ocupados por el *código de acceso.* Se utiliza un código de acceso para identificar la piconet. Cada dispositivo bruto tiene una dirección globalmente única de 6 bytes, de modo que para identificar la piconet se usan los tres bytes menos significativos de la dirección única del maestro. Cuando se forma una trama, cada dispositivo coloca estos bytes en el campo del código de acceso y los complementa con 1/3 de bits FEC (la abreviatura 1/3 especifica que un bit de información se transforma en 3 bits de código). Si el maestro o esclavo recibe una trama que contenga un código de acceso inválido, descarta la trama, pues probablemente ha sido recibida de otra piconet.

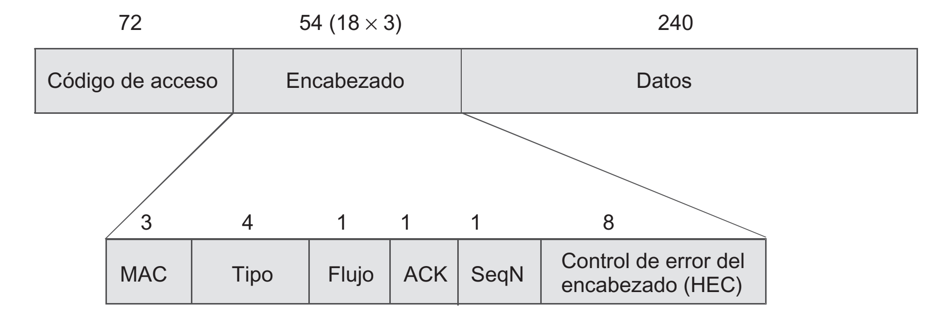


FIGURA 14.16 Formato de una trama Bluetooth que consta de una sola ranura.

- 54 son necesarios para el *encabezado de la trama*, el cual contiene la dirección MAC, una bandera de acuse de recibo de un solo bit, el tipo de trama y algunas otras banderas. La dirección MAC se compone de 3 bits; es la dirección temporal de uno de los siete esclavos, con 000 como una dirección de transmisión. La información del encabezado también es transmitida al usar el código 1/3 FEC.

El formato de una trama que consta de tres o cinco ranuras sólo difiere en el tamaño de su campo de datos. La información colocada en el campo de datos puede ser codificada utilizando 1/3 FEC o 2/3 FEC o puede ser transmitida sin emplear FEC.

14.5.5 Cómo funciona Bluetooth

Considérese un ejemplo de funcionamiento de la piconet. Suponga que esta piconet contiene un maestro y tres esclavos activos. Por sencillez, se puede asumir que todos los dispositivos utilizan tramas que ocupan una sola ranura. La figura 14.17 muestra cómo el maestro distribuye las ranuras entre los miembros de la piconet.

Para asegurar el modo full-dúplex de información, el maestro siempre asigna dos ranuras a cada canal: la primera se utiliza para la transmisión de datos desde el maestro hacia el esclavo, mientras que la segunda se emplea para transmitir datos en la dirección inversa.

En el ejemplo mostrado en la figura 14.17 existe un canal SCO entre el maestro y el esclavo 1. Los canales SCO siempre tienen asignado un ancho de banda fijo, lo cual depende del método FEC adoptado para codificar la información de voz.

1. Si no se utiliza FEC, cada tercer par de ranuras será asignado al canal SCO, como se muestra en la figura. Esta distribución de ranura asegura la transmisión de flujos de 64 Kbps en cada dirección, lo cual se puede verificar. El códec PCM muestrea los datos de voz a 8 KHz (un periodo de 125 μseg) y representa cada muestra con 1 byte. Cada trama lleva 30 bytes (es decir, 240 bits o 30 muestras). Las tramas de los canales SCO transmitidas en una dirección se repiten cada seis ranuras, de modo que el periodo entre tramas es de $6 \times 625 = 3\,750$ μseg. En consecuencia, la tasa o velocidad de información del canal (en una dirección) es de $240/(3\,750 \times 10^{-6}) = 64$ Kbps.
2. Cuando se utiliza codificación 2/3 FEC, el campo de datos de la trama contiene 20 muestras en lugar de 30, de manera que para asegurar una velocidad de 64 Kbps debe asignarse un canal SCO para cada segundo par de ranuras.

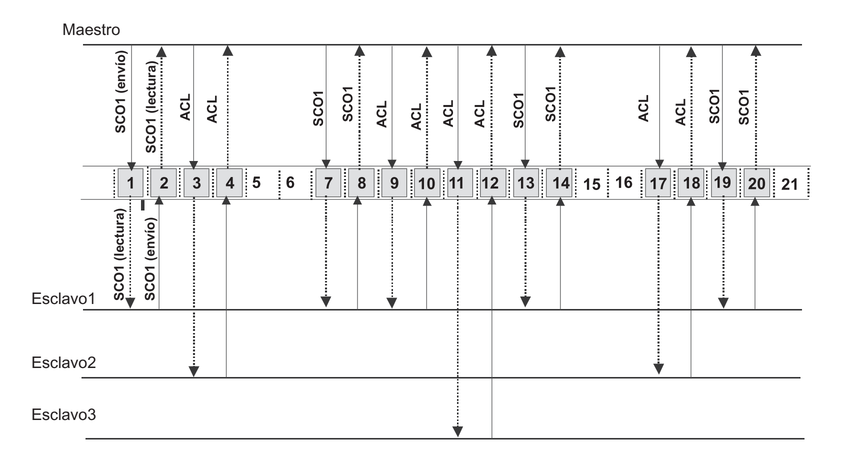


FIGURA 14.17 Compartir el medio.

3. Finalmente, la codificación 1/3 FEC produce una trama que transmite solamente 10 muestras de voz, ocupando todas las ranuras del medio compartido.

Estos cálculos muestran que no pueden existir más de tres canales SCO dentro de una piconet (posiblemente, con distintos dispositivos esclavos); no obstante, esto es posible sólo cuando el canal no emplea codificación FEC para reducir errores de bit. El empleo de FEC reduce el número de canales SCO a dos o incluso a uno.

El ancho de banda restante después de organizar los canales SCO se utiliza para transmitir datos asincrónicos. Para este propósito, la piconet utiliza el canal ACL, que es un canal de punto a multipunto que conecta el maestro a todos los esclavos activos de la piconet. No hay necesidad de establecer este canal, pues existe en cualquier caso.

El maestro polea o sondea de manera periódica los dispositivos esclavos para averiguar si necesitan transmitir datos asincrónicos. Para hacer esto, utiliza una trama POLL especial que contiene la dirección MAC del dispositivo específico. Si el maestro tiene datos para este dispositivo, podrá combinar la transmisión de datos y el poleo dentro de una sola trama.

La figura 14.17 revela que el maestro ha utilizado las ranuras 3 y 4 para intercambiar tramas con el esclavo 2. Las ranuras 9 y 10 fueron utilizadas para intercambio con el esclavo 1, mientras que las ranuras 11 y 12 para intercambio con el esclavo 3. El método de poleo elimina las colisiones cuando se tiene acceso al canal ACL; sin embargo, la velocidad de acceso a este canal no es fija, sino que depende del número de dispositivos que necesiten transmitir datos asincrónicos.

De este modo, las redes Bluetooth combinan conmutación de circuitos (para canales SCO) y conmutación de paquetes (para el canal ACL).

Si los canales SCO no son utilizados en una red Bluetooth, el ancho de banda completo será asignado al canal ACL. Cuando se emplean tramas consistentes en cinco ranuras, la velocidad máxima de transmisión de datos es de 432.6 Kbps en cada dirección (sin usar FEC). También es posible la división asimétrica del ancho de banda del canal ACL, en cuyo caso la velocidad máxima alcanza 723.2 Kbps en una dirección y 57.6 Kbps en la dirección inversa. Éstas son las velocidades del canal ACL, no las velocidades de datos del flujo desde un dispositivo específico. Cuando varios dispositivos comparten el canal ACL, esta velocidad se divide entre todos los dispositivos involucrados.

14.6 EQUIPO PARA LAN DE MEDIOS COMPARTIDOS

PALABRAS CLAVE: tarjeta de interfaz de red (NIC, Network Interface Card), concentrador, adaptador de red, sistema de cableado, medio compartido, LAN, conmutador, puente, enrutador, repetidor de dos puertos, repetidor Ethernet de puertos múltiples, RJ-45, enlaces de reserva, rastreo no autorizado de la red, protección de datos, concentrador de segmento múltiple, conmutación de configuración, concentradores con número fijo de puertos, concentrador modular, concentrador de pila y concentrador de pila modular.

Los concentradores que cuentan con adaptadores de red y sistemas de cableado representan el mínimo de equipo requerido con el cual es posible crear una LAN de medio compartido. Como es evidente, dicha red no puede ser demasiado grande, porque el medio compar-

tido se convierte en un cuello de botella cuando el número de nodos en la red crece de manera significativa. Por ende, los concentradores y los adaptadores de red permiten construir pequeños fragmentos básicos de las redes, que después se unen mediante switches, puentes y ruteadores.

14.6.1 Funciones principales de los adaptadores de red

Junto con su controlador, la **tarjeta de interfaz de red (NIC)** implementa la segunda capa de enlace de datos del modelo OSI en el nodo final de la red (la computadora). Más precisamente, en el sistema operativo de la red, el par adaptador-controlador lleva a cabo únicamente funciones de la capa física y de la capa MAC; a su vez, las funciones de la capa LLC suelen estar implementadas por el módulo OS común a todos los controladores y adaptadores de la red. Por ejemplo, en Windows XP, la capa LLC está implementada en el módulo de especificación de interfaz del controlador de la red (NDIS) común a todos los controladores de NIC, de manera independiente de la tecnología soportada por controladores específicos.

El adaptador de la red y su controlador llevan a cabo dos operaciones en conjunto: recepción y transmisión de tramas.

La *transmisión de la trama* desde la computadora hacia el cable consta de las siguientes etapas:

- Recepción de la trama LLC a través del interfaz de servicio, con la información de la dirección de la capa MAC. Dentro de una computadora, los protocolos interactúan por lo común al usar búferes de la RAM. Los protocolos de capa superior recuperan los datos que se transmitirán a través de la red desde un disco o desde el caché del archivo al utilizar el subsistema de entrada/salida del sistema operativo y al cargar posteriormente los datos en búferes de RAM.
- Formato de la trama de la capa MAC, en el cual la trama LLC es encapsulada. Esto incluye rellenar las direcciones fuente y de destino, así como el cálculo de la suma de verificación.
- Formar símbolos de código, a condición de que se utilicen códigos redundantes como el 4B/5B y aleatorizar códigos para obtener un espectro de señales más uniforme. No todo protocolo implementa esta etapa, por ejemplo: Ethernet de 10 Mbps lo hace sin ella.
- Transmisión de la señal en el cable de acuerdo con el código de línea adoptado: Manchester, NRZI, MLT-3, etcétera.

La *recepción de la trama* desde el cable incluye las etapas siguientes:

- Recepción de las señales del cable codificando el flujo de bits.
- Separación de las señales del ruido, lo cual puede realizarse mediante circuitos especiales o procesadores de señales digitales. Como resultado, el receptor del adaptador obtiene una secuencia de bits con una alta probabilidad de coincidir con la secuencia enviada por el transmisor.
- Paso de los datos a través de un desaleatorizador o descifrador si aquéllos hubieran sido aleatorizados antes de ser enviados. Después de esta operación, los símbolos de código enviados por el transmisor se restablecen en el adaptador.
- Comprobación de la suma verificadora de la trama. Si dicha suma es incorrecta se descartará la trama y se pasará un código de error específico al protocolo LLC a través de la interfaz del servicio. Si la suma verificadora es correcta, la trama LLC se recuperará desde la trama MAC y se pasará al protocolo LLC a través de la interfaz del servicio.

Los estándares no definen la distribución de responsabilidades entre el adaptador y su controlador; por lo tanto, cada fabricante es libre de resolver este problema. Como regla, los adaptadores de red están clasificados en dos categorías: adaptadores para computadoras cliente y adaptadores para servidores.

En los adaptadores para *computadoras cliente*, la mayoría del trabajo se delega al controlador. De este modo, el adaptador se hace menos complejo y su precio es bastante menor. La desventaja de este enfoque es una carga excesiva sobre el CPU, el cual en este caso debe realizar operaciones de rutina tales como la transmisión de la trama desde los búferes de RAM hacia la red.

Los adaptadores proyectados para *servidores* están equipados con procesadores integrados que llevan a cabo la mayoría de las tareas relacionadas con la transmisión de la trama desde la RAM hacia la red y viceversa.

Con base en el protocolo implementado por el adaptador se clasifican como adaptadores de Ethernet, adaptadores de Token Ring, adaptadores FDDI, etc. Como Fast Ethernet permite usar autonegociación para seleccionar la velocidad de operación del adaptador de la red de manera automática, según las capacidades del concentrador, muchos adaptadores Ethernet ahora soportan dos velocidades de operación y tienen el prefijo 10/100 en sus nombres.

Los adaptadores de red implementan el método de canalización o encausamiento (pipeline) del procesamiento de la trama. De acuerdo con este método, los procesos recepción de la trama desde la RAM de la computadora y la transmisión de la trama en la red ocurren en paralelo. Así, una vez recibidos varios bytes de inicio de la trama, el adaptador comienza a transmitirlos. Esto aumenta (en 25-55%) el rendimiento de la cadena *RAM-adaptador-enlace físico-adaptador-RAM* de manera considerable. Dicho método es muy sensible al umbral del inicio de la transmisión (es decir, al número de bytes de la trama que deben ser cargados en el búfer del adaptador antes de comenzar la transmisión real). Los adaptadores de red realizan el autoajuste de este parámetro al analizar el medio y calcular el valor de umbral sin la participación del administrador de la red. La autoconfiguración asegura un rendimiento máximo para combinaciones específicas del bus interno de la computadora y sus configuraciones de IRQ y DMA.

Los adaptadores de la red están basados en circuitos integrados de aplicaciones específicas (ASIC, por sus siglas para Application-Specific Integrated Circuits), los cuales mejoran tanto su rendimiento como su confiabilidad, al mismo tiempo que reducen sus costos.

NOTA *Es importante la velocidad de operación mejorada del canal entre la memoria y el adaptador para un incremento global del rendimiento de la red, pues la velocidad de transmisión de la trama sobre una ruta compleja —que puede incluir, por ejemplo, concentradores, conmutadores, enrutadores y enlaces WAN— siempre depende del rendimiento de su elemento más lento. Por lo tanto, si el adaptador de red del servidor o del cliente funciona con lentitud, incluso los dispositivos de comunicación de red más rápidos serán incapaces de incrementar la velocidad de operación global de la red.*

Los adaptadores de red fabricados en la actualidad pueden ser clasificados como adaptadores 4G (de cuarta generación). Deben incluir el chip del circuito integrado de aplicaciones específicas (ASIC), el cual lleva a cabo las funciones de la capa MAC, además de muchas funciones de alto nivel. El conjunto de tales funciones puede incluir soporte para un agente de monitoreo remoto, métodos para dar prioridad a las tramas y funciones de control remoto. Los adaptadores de red dirigidos a servidores casi siempre contienen un poderoso procesador integrado, el cual reduce la carga sobre el CPU.

14.6.2 Funciones principales de los concentradores

Prácticamente todas las tecnologías de LAN contemporáneas definen un dispositivo que tiene tres nombres que se utilizan de modo intercambiable: *concentrador*, *"hub"* (*"concentrador"*, *en inglés*) y *repetidor.* Según el área de aplicación, su diseño y el conjunto de sus funciones pueden variar considerablemente. Sólo su función principal permanece sin cambios: *repetir la trama* en todos sus puertos (como se define en el estándar Ethernet) o solamente en ciertos puertos, de acuerdo con el algoritmo definido por el estándar relevante.

Por lo regular, el concentrador tiene varios puertos a los cuales se conectan los nodos terminales de la red y las computadoras utilizando segmentos de cable físico por separado. El concentrador conecta segmentos físicos de la red en un medio compartido común, al que se realiza el acceso de acuerdo con uno de los protocolos LAN anteriormente considerados: Ethernet, Token Ring, etc. Como el acceso lógico al medio compartido depende en gran medida de la tecnología, se fabrican concentradores especiales para todas las tecnologías populares.

Cada concentrador realiza una *función especial* definida en el estándar apropiado de la tecnología que soporta.

Aparte de la función principal, el concentrador puede efectuar varias *funciones adicionales* que pueden no estar definidas en los estándares o ser capacidades opcionales. Por ejemplo, el concentrador de Token Ring puede desconectar de manera incorrecta puertos de operación y conmutar al anillo de reserva, aunque el estándar no describe dichas capacidades funcionales. Los concentradores probaron ser dispositivos convenientes para llevar a cabo funciones auxiliares que simplifican el mantenimiento y control de la red.

Considérense las características de implementación específicas de la función principal del concentrador en un ejemplo de concentradores de Ethernet.

En Ethernet, los dispositivos que conectan varios segmentos físicos de cable coaxial en un solo medio compartido se utilizaron por largo tiempo. Basados en su función principal (repetir en todos los puertos de salida las señales recibidas en uno de sus puertos de entrada), estos dispositivos llegaron a ser conocidos como *repetidores Ethernet*. En redes basadas en cable coaxial, eran más comunes los **repetidores de dos puertos**, conectando solamente dos segmentos de cable. Por esta razón, el término *concentrador* rara vez se aplica a ellos.

Con la adopción del par trenzado en 10Base-T, los repetidores llegaron a ser una parte integral de las redes Ethernet, pues sin ellos las comunicaciones solamente podían organizarse entre dos nodos de la red. Los **repetidores Ethernet de puertos múltiples** basados en un par trenzado llegaron a conocerse como concentradores o "hubs", porque un solo dispositivo concentraba las conexiones entre un gran número de nodos de red. La figura 14.18 muestra un concentrador Ethernet típico proyectado para crear segmentos pequeños en un medio compartido. Tiene 16 puertos 10Base-T con conectores RJ-45 y un solo puerto AUI para conectar un transceptor externo. Como regla, un transceptor que utiliza cable coaxial o fibra óptica se conecta a este puerto. Con este transceptor, el concentrador se conecta a un cable troncal que conecta varios concentradores. Las estaciones localizadas a 100 m o más lejos del concentrador están conectadas de la misma manera.

NOTA *Para conectar concentradores 10Base-T en un sistema jerárquico, pueden emplearse los mismos puertos que aquellos que conectan estaciones de trabajo del usuario final. Sin embargo, existe una circunstancia específica que debe ser tomada en cuenta en un sistema de esta clase: un puerto RJ-45 normal destinado a conectar un adaptador de red y denominado interfaz dependiente del medio con entrecruzamiento (crossover) (MDI-X, donde la X significa crossover o entrecruzamiento) tiene el arreglo inverso de los contactos del conector para hacer posible conectar un adaptador de*

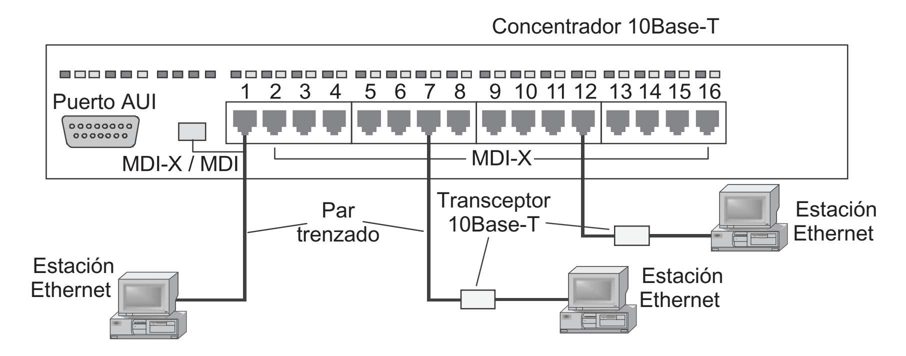


FIGURA 14.18 Concentrador Ethernet.

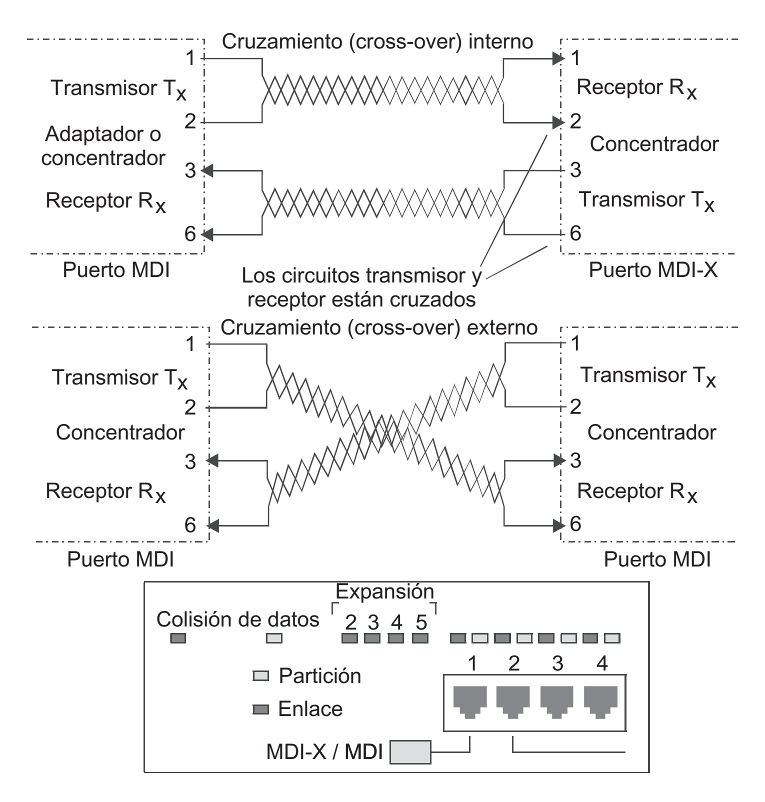


FIGURA 14.19 Conexiones estación-concentrador y concentrador-concentrador basadas en par trenzado.

red al concentrador utilizando un cable de conexión estándar, el cual no cruza los contactos (figura 14.19). Cuando los concentradores están conectados mediante un puerto MDI-X estándar, es necesario emplear cable no estándar con pares conectados en forma entrecruzada. Por ende, algunos fabricantes suministran el concentrador con un puerto MDI delicado, el cual no utiliza entrecruzamiento de pares. De este modo, dos concentradores pueden ser conectados de manera normal: directamente a través del cable usando el puerto MDI-X de un concentrador y el puerto MDI del otro. A menudo, el mismo puerto del concentrador puede funcionar tanto como un puerto MDI-X y como un puerto MDI, lo cual depende de la posición del contacto de conmutación, como se muestra en la parte inferior de la figura 14.19.

Se puede considerar un repetidor-concentrador Ethernet de puerto múltiple desde diferentes posiciones cuando se aplica la **regla de los cuatro nodos**. En la mayoría de los modelos, todos los puertos están conectados a una sola unidad repetidora; en consecuencia, cuando la señal pasa entre dos puertos, la unidad repetidora introduce el retardo solamente una vez. Por lo tanto, un concentrador así debe ser considerado un repetidor simple que impone limitaciones de acuerdo con la regla de los cuatro nodos. No obstante, otros modelos de repetidores tienen varios puertos con sus unidades repetidoras; en este caso, cada unidad repetidora debe ser considerada un repetidor simple y tenerse en cuenta por separado cuando se aplique la regla de los cuatro nodos.

Sin embargo, en contraste con las diferencias en la implementación de las funciones del concentrador principal, las cuales son insignificantes, las diferencias al poner en práctica las funciones auxiliares en los concentradores son considerables.

14.6.3 Autoparticionamiento

El **autoparticionamiento** es una función útil del concentrador que permite a éste desconectar puertos que funcionan de manera incorrecta. Ayuda a aislar las otras partes de la red de problemas que surjan en el nodo con funcionamiento incorrecto.[4] La principal razón para la desconexión del puerto en los estándares Ethernet y Fast Ethernet es la ausencia de respuesta a la secuencia de pulsos de prueba de enlace enviados a todos los puertos cada 16 milisegundos. En este caso, el puerto con mal funcionamiento es conmutado al estado de desconexión; no obstante, continuarán enviándose pulsos de prueba de enlace hacia el puerto, de manera que cuando el dispositivo se restablezca continuará en funcionamiento de manera automática.

Considere las situaciones en las cuales los concentradores de Ethernet y Fast Ethernet desconectan los puertos:

- *Errores a nivel de la trama.* Si la intensidad de las tramas erróneas que pasan a través del puerto exceden el umbral predefinido, el puerto se desconecta. Luego, a condición de que no haya errores durante los espacios predefinidos, el puerto se conecta de nuevo. Tales errores pueden incluir una suma verificadora incorrecta, una longitud de trama inválida (más de 1 518 bytes o menos de 64 bytes) o un encabezado de trama erróneo.
- *Colisiones múltiples.* Si el concentrador registra que el mismo puerto fue la fuente de colisión más de 60 veces, el puerto se desconectará. Después de cierto tiempo, el puerto se conectará otra vez.
- *Transmisión prolongada (jabber o bailoteo).* Como un adaptador de red, el concentrador controla el tiempo durante el cual una trama simple pasa a través del puerto. Si este tiempo excede el intervalo requerido para transmitir una trama de la longitud máxima más de tres veces, el puerto se desconectará.

14.6.4 Soporte de enlaces de reserva

Como el uso de enlace de reserva en los concentradores está definido sólo en FDDI, los diseñadores del concentrador dieron soporte de esta función en concentradores dirigidos a

[4] En concentradores FDDI, esta función es la principal para la mayoría de las situaciones de error, pues está definida en el protocolo.

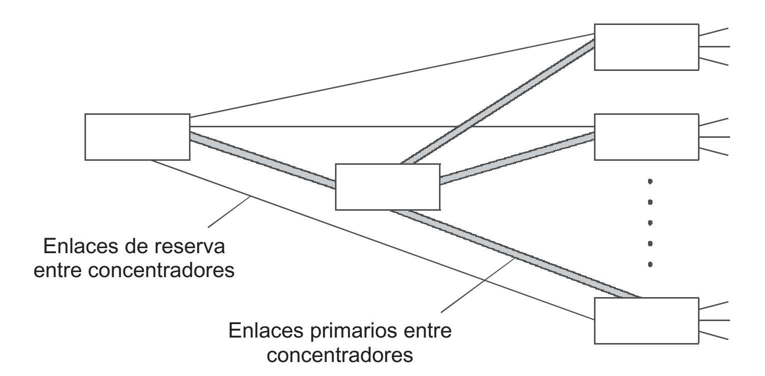


FIGURA 14.20 Enlaces de reserva entre concentradores Ethernet.

otras tecnologías únicamente como una opción. Por ejemplo, los concentradores de Ethernet pueden formar sólo enlaces jerárquicos sin ciclos o "loops". Por lo tanto, los enlaces de reserva solamente pueden existir entre puertos desconectados para evitar violaciones a la lógica de funcionamiento de la red. Por lo regular, cuando se configura un concentrador, el administrador de la red debe determinar cuáles son los puertos principales y cuáles son puertos de reserva (figura 14.20). Si el puerto es desconectado por alguna razón (es decir, el mecanismo de autoparticionamiento entra en acción), el concentrador activará su puerto de reserva.

En algunos modelos de concentrador, el uso del mecanismo de reservación del puerto se permite sólo para los enlaces más importantes basados en cable de fibra óptica. En algunos otros modelos, es posible reservar cualquier puerto.

14.6.5 Protección contra acceso no autorizado

Los medios compartidos hacen sencilla la intromisión y el acceso de datos transmitidos, sin tener autorización en la red. Para conseguir esto, es suficiente conectar una computadora instalada con una copia del analizador de protocolo a un conector de concentrador libre y grabar todo el tráfico que pasa por la red en un archivo en el disco duro. Después de ello, es posible recuperar toda la información requerida.

Los fabricantes de concentradores proporcionan algunos métodos para proteger los datos en medios compartidos.

El método de protección más simple es asignar direcciones MAC permitidas a los puertos del concentrador. En un concentrador Ethernet estándar, los puertos no tienen direcciones MAC. La protección de los datos consiste en asignar manualmente direcciones MAC específicas a cada puerto del concentrador. Esta dirección MAC es la de la estación permitida para conectarse a ese puerto; por ejemplo, en la figura 14.21, el primer puerto del concentrador tiene asignada una dirección MAC específica (convencionalmente, 123). La computadora con la dirección MAC equivalente puede comunicarse de manera normal con la red al usar ese puerto. Si un intruso desconecta esa computadora y conecta alguna otra, el concentrador notará que después de que arranca la nueva computadora, la dirección fuente de las tramas que llegan hacia la red desde la nueva computadora habrá cambiado (por ejemplo, a 789). Como esta dirección es inválida para el primer puerto, estas tramas son eliminadas, el puerto es desconectado y se puede registrar un incidente de seguridad.

Para implementar este método de protección de datos del concentrador, es necesario configurar el concentrador; para ello, el concentrador ha de estar equipado con una unidad

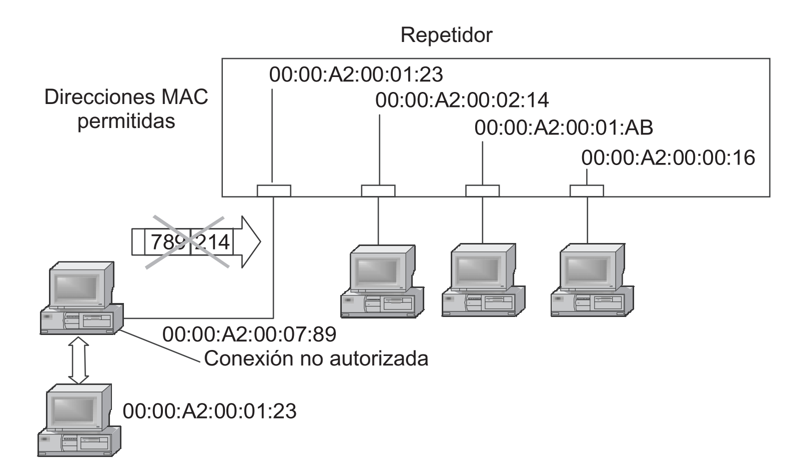


FIGURA 14.21 Aislamiento del puerto: la transmisión de las tramas se permite solamente desde las estaciones con direcciones MAC predefinidas.

de control. Tales concentradores generalmente son denominados *concentradores intelectuales*. La unidad de control es una unidad de cálculo compacta con software integrado. Para asegurar que el administrador puede comunicarse con la unidad de control, el concentrador tiene un puerto de consola (con mucha frecuencia el puerto RS-232) al cual se conecta una terminal o una PC instalada con un programa de emulación de terminal. Cuando la terminal se conecta al puerto de consola, la unidad de control exhibe un diálogo, mediante el cual el administrador de la red puede introducir direcciones MAC. La unidad de control puede soportar otras operaciones de configuración, como conexión o desconexión manual de puertos. Con este propósito, la unidad de control muestra alguna forma de menú en la pantalla de la terminal. Mediante el uso de este menú, el administrador de la red puede seleccionar la acción requerida.

Otro método para proteger los datos contra accesos no autorizados es la encriptación en el concentrador. No obstante, la encriptación auténtica requiere potencia de cómputo significativa. Por lo tanto, para concentradores sin almacenamiento temporal ("buffering") de tramas, es bastante problemático hacer la encriptación de los datos al vuelo. En lugar de la encriptación auténtica, los concentradores usan distorsión aleatoria del campo de los datos en los paquetes transmitidos hacia los puertos con direcciones diferentes de la dirección de destino del paquete. Este método conserva la lógica del acceso aleatorio al medio, pues todas las estaciones pueden notar que el medio está ocupado con la transmisión de una trama de información. Sin embargo, sólo la estación de destino a la cual se dirige la trama que se transmitió puede interpretar de manera correcta el contenido de su campo de datos (figura 14.22). Para implementar este método se deben suministrar al concentrador las direcciones MAC de todas las estaciones conectadas a sus puertos. Por lo regular, los campos de datos en las tramas enviadas a las otras estaciones aparte de los nodos de destino se llenan con ceros.

14.6.6 Concentradores de segmentos múltiples

¿Por qué algunos modelos de concentradores son equipados con un gran número de puertos, digamos 192 o 240?, ¿tiene algún sentido dividir un medio de 10 o 16 Mbps entre un número tan grande de estaciones? Hace 10 o 15 años, la respuesta en algunos casos podría haber sido sí. Por ejemplo, esto es verdadero para las redes cuyas computadoras utilizan el

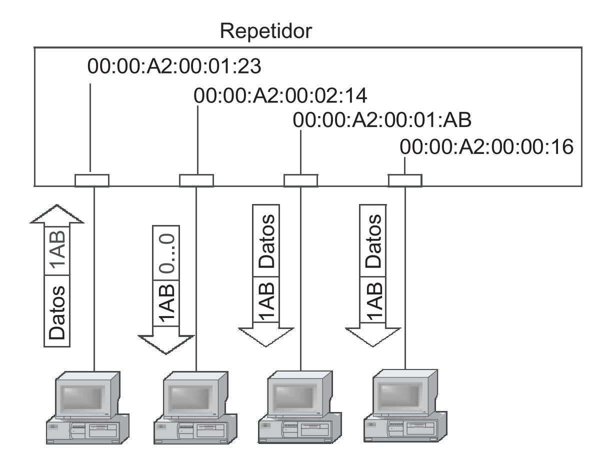


FIGURA 14.22 Distorsión en el campo de datos en las tramas no destinadas para recepción por las estaciones.

medio sólo para enviar pequeños mensajes de correo o copiar pequeños archivos de texto. En la actualidad, no hay muchas redes así e incluso cinco computadoras pueden cargar completamente un segmento de Ethernet.

> Entonces, ¿por qué es necesario un concentrador con un número de puertos tan grande, en especial si en la práctica es casi imposible utilizar todos los puertos debido a las limitaciones en el ancho de banda por estación?

La respuesta reside en que tales concentradores tienen varios buses internos que no están interconectados, sino que se hallan destinados a crear varios medios compartidos. Por ejemplo, el concentrador ilustrado en la figura 14.23 tiene tres buses Ethernet internos. Si un concentrador así tiene 72 puertos, cada uno de ellos podrá esta conectado a cualquiera de los tres buses. La configuración en la figura 14.23 muestra que las primeras dos computadoras están conectadas al bus Ethernet 3, mientras que la tercera y cuarta estaciones se encuentran conectadas al bus Ethernet 1. Las primeras dos computadoras forman un segmento compartido, mientras que la tercera y cuarta estaciones forman otro.

Las computadoras conectadas a diferentes segmentos no pueden comunicarse mediante el uso del concentrador, pues sus buses internos no están interconectados.

Los concentradores de segmentos múltiples son necesarios para conectar segmentos compartidos que pueden ser cambiados con facilidad. La mayoría de los concentradores de segmento múltiple pueden realizar la conexión del puerto a uno de sus buses internos de manera programada, por ejemplo: mediante configuración local al usar un puerto de consola. Como resutado, el administrador de la red puede conectar las computadoras de los usuarios a cualquier puerto del concentrador y posteriormente controlar la estructura de cada segmento empleando el programa de configuración del concentrador. Por ejemplo, si el segmento 1 se llega a congestionar, sus computadoras podrán distribuirse entre los segmentos restantes del concentrador.

> El cambio de manera programada entre los puertos y los buses internos del concentrador se conoce como **conmutación de configuración**.

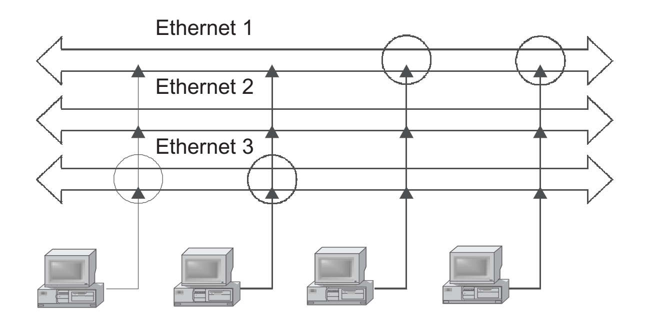


FIGURA 14.23 Concentrador multisegmentos.

NOTA *La conmutación de configuración no tiene nada en común con la conmutación de paquete realizada por medio de puentes y conmutadores.*

Los concentradores de segmento múltiple forman una base programable para redes a gran escala. Los segmentos interconectados requieren emplear otros dispositivos: puentes, conmutadores o enrutadores. Tales dispositivos entre redes deben conectarse a varios puertos de un concentrador de segmentos múltiples vinculado con diferentes buses internos. El objetivo principal de un dispositivo de esta clase es transportar tramas o paquetes entre segmentos como si ellos fueran creados utilizando concentradores por separado.

Para una red a gran escala, un concentrador de segmentos múltiples desempeña el papel de un estante intelectual, el cual crea una nueva conexión de manera programada mediante el cambio de la configuración del dispositivo interno en vez de conectar de manera mecánica el enchufe del cable a otro puerto.

14.6.7 Diseño del concentrador

El área de aplicación del concentrador ejerce una influencia considerable en su diseño. Los concentradores de grupos de trabajo por lo regular se liberan como dispositivos con un número fijo de puertos, mientras que los concentradores corporativos son dispositivos modulares basados en un chasís. Los concentradores de nivel departamental pueden tener una estructura de pila. Una división así no es rígida y los concentradores modulares también pueden utilizarse como dispositivos de nivel corporativo.

Los **concentradores con un número fijo de puertos** tienen el diseño más simple. Un dispositivo de esta clase es una unidad separada con todos los elementos requeridos (puertos, indicadores, controles y una fuente de energía). Estos elementos no pueden ser reemplazados. Por lo general, todos los puertos de un concentrador así soportan un medio de transmisión; el número total de puertos varía entre 4 y 48; a su vez, un puerto puede estar dedicado a conectar al concentrador al troncal de la red o a enlazar concentradores. (Con mucha frecuencia, el puerto AUI se utiliza para dicho propósito: en este caso, el uso de un transceptor apropiado permite que el concentrador sea conectado prácticamente a cualquier medio de transmisión físico.)

Los **concentradores modulares** están implementados como módulos separados con un número fijo de puertos instalados en un chasís común. El chasís tiene un bus interno para enlazar módulos separados en un repetidor común. A menudo tales repetidores son de segmentos múltiples, en cuyo caso existen varios repetidores no interconectados dentro de un solo concentrador modular. Pueden existir varios tipos de módulos para un concentrador

modular, que difieren en el número de puertos y el medio físico soportado. Los concentradores modulares permiten tanto la configuración del concentrador para seleccionarse con más precisión, como reacciones flexibles, de bajo costo, a los cambios de configuración de la red.

Debido a que los concentradores modulares corporativos llevan a cabo tareas cruciales, están equipados con una unidad de control, un sistema de control térmico, unidades redundantes de suministro de energía y la posibilidad de reemplazar módulos de manera espontánea.

El alto costo es la desventaja más importante de los concentradores basados en chasís cuando una empresa necesita instalar solamente uno o dos módulos en la etapa inicial del despliegue de la red. El chasís es costoso porque se suministra con todos los otros dispositivos, tal como las unidades redundantes de suministro de energía. Por lo tanto, los **concentradores de pila** se han convertido en la opción más popular para las redes de dimensiones medias.

Los concentradores en pila, como los concentradores con un número fijo de puertos, se suministran en la forma de unidades separadas sin la posibilidad de reemplazar los módulos individuales. Ejemplos típicos de diversos concentradores de pila Ethernet se muestran en la figura 14.24.

Los concentradores de pila tienen puertos y cables especiales para conectar varias de esas unidades en un repetidor simple (figura 14.25) que tiene una unidad repetidora común, asegura la resincronización global de la señal y, por consiguiente, puede considerarse un repetidor simple en términos de la regla de los cuatro nodos. Si los concentradores de pila tienen varios buses internos, éstos se enlazan y llegan a ser comunes a todos los dispositivos de pila cuando enlazan estos concentradores a la pila. El número de dispositivos unidos a la pila puede ser muy grande (normalmente hasta ocho, pero en ocasiones incluso más). Los concentradores de pila pueden soportar varios medios de transmisión físicos, lo que los hace casi tan flexibles como los concentradores modulares; sin embargo, el costo de los concentradores de pila por puerto es generalmente más bajo, pues una empresa puede comenzar con un solo dispositivo sin un chasís redundante y después agregar dispositivos semejantes a la pila a medida que sea necesario.

Los concentradores de pila del mismo fabricante por lo regular tienen el mismo diseño, lo que hace fácil su instalación en forma apilada, uno encima del otro, formando así un solo dispositivo de escritorio, o colocarlos en un chasís común. Cuando se organiza una pila, también es posible economizar en la unidad de control común a todos los dispositivos de la pila;

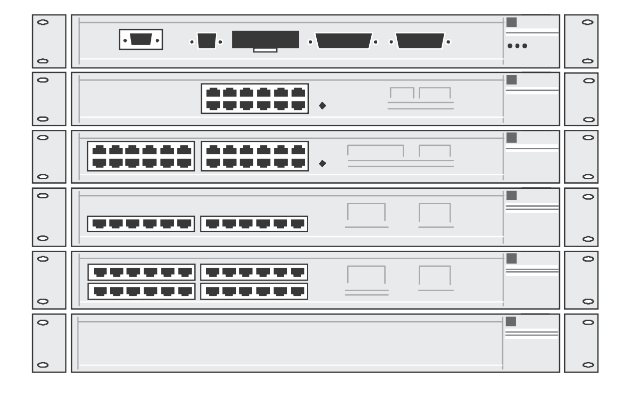


FIGURA 14.24 Concentradores de pila Ethernet.

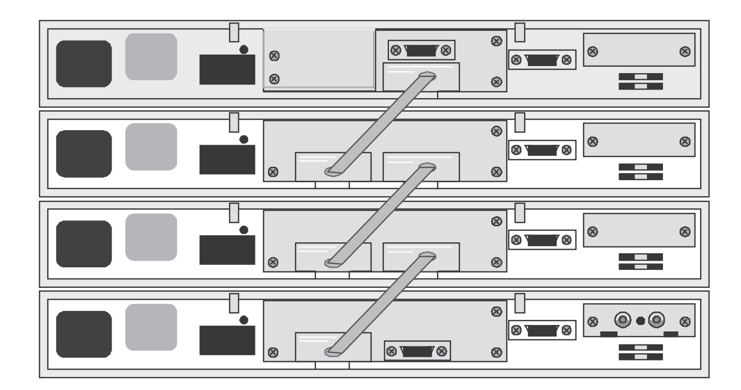


FIGURA 14.25 Conexión de concentradores de pila en un dispositivo simple con el uso de conectores especiales en el panel posterior.

puede insertarse como un módulo agregado en el chasís común. Será factible un potencial de ahorro adicional si se usa una unidad redundante de suministro de energía común.

Los **concentradores de pila modulares** son concentradores modulares enlazados en la pila utilizando enlaces especiales. Como regla, esos estuches de concentrador están proyectados para un número pequeño de módulos (1 a 3). Estos concentradores combinan las ventajas de ambos tipos de concentradores.

Tal clasificación de diseños de concentrador es aplicable no solamente a los concentradores, sino también a otros tipos de dispositivos de comunicación: los puentes y enrutadores de LAN y los conmutadores y enrutadores de WAN. No todos los tipos de dispositivos implican tan cercana interacción entre los elementos de la pila como los concentradores. Con frecuencia, los dispositivos de pila están enlazados únicamente por unidades de suministro de energía y unidades de control en común; las funciones principales se llevan a cabo de manera autónoma por cada dispositivo de la pila.

RESUMEN

- Las redes Token Ring utilizan acceso determinístico para implementar la señal circulante. Este método garantiza que cada estación tenga acceso al anillo compartido durante el tiempo de intercambio de la señal. La topología lógica de un Token Ring es un anillo y la topología física de una red así es de estrella.
- Las redes Token Ring funcionan a dos velocidades (4 y 16 Mbps) y pueden utilizar par trenzado con protección de blindaje o sin ella, además de cables de fibra óptica como un medio de transmisión. El número máximo de estaciones en el anillo es de 260 y la longitud máxima del anillo es de 4 km. El uso de la topología de anillo permite a las redes Token Ring asegurar características básicas de tolerancia a las fallas.
- La sucesión de Token Ring a FDDI es bastante significativa: ambas utilizan la misma topología de red y también señales circulantes como el método de acceso; a su vez, FDDI soporta herramientas avanzadas de tolerancia a las fallas. En caso de fallas aisladas del sistema de cableado o de una de las estaciones de trabajo del anillo, la red preserva la funcionalidad al envolver el anillo actual en uno solo.
- La interfaz de datos distribuidos por fibra óptica (FDDI) fue la primera tecnología en emplear cables de fibra óptica en LAN y asegurar transmisión de datos a 100 Mbps.

- El número máximo de estaciones con una conexión doble en un anillo FDDI es de 500; el diámetro máximo de un anillo dual es de 100 km. Esto hace a FDDI apropiado para su uso no solamente en las LAN, sino también en las MAN.
- Las LAN inalámbricas prescinden del engorroso sistema de cableado y aseguran la movilidad del usuario. Sin embargo, requieren que los arquitectos de la red resuelvan un conjunto de complicados problemas relacionados con el alto nivel de características de ruido de los medios inalámbricos y una zona de cobertura de red indefinida.
- Los estándares IEEE 802.11 son los más prometedores para las LAN inalámbricas. Existen diversas variantes de las especificaciones de la capa física 802.11, que difieren en términos del intervalo de frecuencia (2.4 o 5 GHz) y método de codificación (FHSS, DSSS u OFDM). La capa física 802.11b asegura la transmisión de datos de hasta 11 Mbps.
- El método de acceso 802.11 es una combinación de acceso aleatorio con prevención de colisiones y acceso determinístico centralizado basado en poleo (sondeo). El primer modo está implementado mediante algoritmos de función de coordinación distribuida (DCF) y el segundo modo mediante algoritmos de función de coordinación de punto (PCF).
- El uso flexible de DCF y PCF permite contar con el soporte QoS para el tráfico sincrónico y asincrónico.
- Las redes de área personal (PAN) están proyectadas para organizar la interacción entre dispositivos pertenecientes a un solo propietario a través de distancias pequeñas (por lo regular, de 10 a 100 metros). Las PAN deben asegurar el acceso tanto fijo como móvil, por ejemplo: dentro de un edificio o cuando el usuario se mueve entre habitaciones, edificios o ciudades.
- En la actualidad, Bluetooth es la tecnología PAN más popular y utiliza el concepto de piconet. Una piconet puede incluir hasta 255 dispositivos, pero únicamente ocho pueden estar activos e intercambiar datos en cualquier momento. Uno de los dispositivos piconet es el maestro; los otros dispositivos son esclavos.
- Diversas piconets localizadas en la misma área y que efectúan intercambio de datos forman una scatternet. Las piconets que forman una scatternet interactúan entre sí por medio de un nodo simple (puente) que forma parte de varias piconets de manera simultánea.
- Para el tráfico sensible al retardo, las redes Bluetooth soportan enlaces sincrónicos orientados a la conexión (SCO); para el tráfico elástico utilizan enlaces asincrónicos sin conexión (ACL). Los enlaces SCO se utilizan normalmente para transmitir tráfico de voz a 64 Kbps, mientras que los canales ACL son empleados para el tráfico de computadora a velocidades variables de hasta 723 Kbps.
- Aparte de su función principal de protocolo (repetición bit a bit de la trama a todos los puertos o al puerto siguiente), los concentradores de LAN siempre llevan a cabo diversas funciones auxiliares útiles, incluido lo siguiente:
  - Autoparticionamiento, que es una de las más importantes funciones auxiliares, mediante la cual el concentrador podrá desconectar el puerto si detecta problemas con el cable o el nodo extremo conectado a ese puerto.
  - Protección para la red en contra de accesos no autorizados al rechazar la conexión de computadoras con direcciones MAC desconocidas a los puertos del concentrador.

PREGUNTAS DE REPASO

1. Describa el algoritmo de acceso al medio utilizado en Token Ring.
2. ¿Qué funciones lleva a cabo el monitor activo?
3. ¿Por qué las redes Token Ring son capaces de mantener la conectividad si una de las computadoras que forman el anillo se apaga?
4. Especifique los tamaños máximos de campo de datos permitido para:
   - Ethernet.
   - Token Ring.
   - FDDI.
   - Bluetooth.
5. ¿Con qué fundamento se elige el tiempo máximo de intercambio de señal para las redes Token Ring?
6. ¿Cuál elemento de la red Token Ring restablece la sincronización del flujo de bits?
7. ¿Cuáles son las ventajas del mecanismo inicial de liberación de señal?
8. ¿Qué características tienen en común FDDI y Token Ring y de qué manera difieren?
9. ¿Qué elementos de las redes FDDI aseguran la tolerancia a las fallas?
10. FDDI es tolerante a las fallas. ¿Significa esto que en condiciones de ruptura de cualquier cable simple la red puede continuar su funcionamiento normal?
11. ¿Cuáles son las consecuencias de una ruptura de cable duplicada en anillos FDDI?
12. ¿Qué pasa si un cable de una estación de enlace simple (SAS) se daña en una red FDDI?
13. ¿Qué métodos de codificación de señales se utilizan en las redes IEEE 802.11?
14. ¿Qué tipo de medio usa el DS para transmisión de datos entre los BSS?
15. ¿Cuál es la influencia del efecto de terminal oculta?
16. ¿Cómo detecta las colisiones la capa MAC en las redes 802.11?
17. ¿Es posible para una estación perteneciente a una red 802.11 transmitir una trama a otra estación perteneciente a la misma BSS al emplear un AP?
18. ¿Cuál es el propósito de dividir el tiempo permitido para transmisión de trama en ranuras en DCF?, ¿qué debe tenerse en cuenta cuando se elige la duración de la ranura?
19. ¿Por qué PCF siempre tiene prioridad sobre DCF?
20. ¿Cómo se enlazan las piconets de Bluetooth en una scatternet?
21. ¿Por qué no se utilizan todos los 625 bits de una ranura de tiempo Bluetooth para transmisión de la trama?
22. ¿En qué casos puede una trama sencilla de Bluetooth transportar datos de uno, dos o tres canales SCO?
23. ¿Qué métodos de conmutación se utilizan en Bluetooth?
24. ¿Por qué se eligió la arquitectura maestro-esclavo para Bluetooth?
25. ¿Cómo los anchos de banda del adaptador de la red y del concentrador influyen en el rendimiento de la red?
26. ¿Cómo soportan los concentradores los enlaces de reserva?
27. De acuerdo con su función principal (la repetición de una señal), los concentradores se clasifican como dispositivos que funcionan en la capa física del modelo OSI. Proporcione ejemplos de funciones auxiliares del concentrador para las que el concentrador necesita información de protocolos de capa superior.
28. ¿Cuáles son las diferencias entre concentradores modulares y de pila?
29. ¿Por qué se utilizan puertos especiales para la interconexión de concentradores?

PROBLEMAS

1. Evalúe el tiempo máximo de espera para tener acceso al medio en una red Token Ring con 160 estaciones y funcionando a 16 Mbps.
2. Una red Token Ring incluye 100 estaciones. La longitud total del anillo es de 2 000 m y la velocidad de transmisión es de 16 Mbps. El tiempo de retención de la señal se establece en 10 mseg. Cada estación transmite tramas de extensión fija de 4 000 bytes (con el encabezado) y utiliza completamente el tiempo de retención de la señal para transmitir todas sus tramas. Calcule la ganancia producida por el uso del mecanismo inicial de liberación de la señal en esta red.
3. Las redes IEEE 802.11 y Bluetooth funcionan dentro del mismo territorio. La red 802.11 utiliza la especificación de capa física FHSS para la transmisión de datos a 1 Mbps. A su vez, la red Bluetooth funciona con una velocidad estándar de granulación de 1 600 Hz, mientras que la red 802.11 soporta una velocidad de granulación de 50 Hz. Ambas redes emplean 79 canales en el intervalo de los 2.4 GHz.

   Determine la proporción de tramas en cada red que se corrompen debido al uso del mismo canal de frecuencia por ambas redes. Por exactitud, considere que todos los datos en la red Bluetooth se transmiten en tramas de una ranura y que la red 802.11 utiliza tramas de longitud máxima.

15

FUNDAMENTOS DE LAN CONMUTADA

DESCRIPCIÓN DEL CAPÍTULO

15.1 INTRODUCCIÓN

Los medios compartidos se utilizaron en LAN desde que las redes de este tipo aparecieron por primera vez. Un enfoque de tal naturaleza para usar los enlaces de comunicaciones tiene varias ventajas, una de las cuales es la simplicidad del equipo de comunicaciones de la LAN. No obstante, la utilización de un medio compartido no está libre de desventajas. El inconveniente más notorio de las LAN de medios compartidos es la baja escalabilidad, porque un incremento en el número de nodos de la red produce una disminución proporcional en el ancho de banda asignado a cada nodo.

La solución natural al problema de la escalabilidad de la LAN es dividirla en varios segmentos, de tal manera que cada uno representa un medio compartido por separado. Esta partición lógica se lleva a cabo con puentes o switches (interruptores) de LAN. En el capítulo 3 se estudiaron los principios de la estructuración lógica de la red. En este capítulo se analizarán con más detalle los algoritmos de operación de los puentes y switches.

Las LAN divididas en segmentos lógicos se denominan **LAN conmutadas**. Un segmento de red que consta de una computadora directamente conectada al puerto del switch se conoce como **microsegmento**. En esencia, un microsegmento ya no es un medio compartido, sino un canal dúplex utilizado por los transmisores de la computadora o el puerto switch de la forma que sea necesaria sin compartir con los transmisores.

Aunque una LAN conmutada siempre es una solución más costosa que una LAN de medio compartido, asegura varias ventajas aparte de la escalabilidad. Las principales ventajas de las LAN conmutadas se verán en este capítulo.

15.2 ESTRUCTURACIÓN DE REDES LÓGICAS CON EL USO DE PUENTES Y SWITCHES (INTERRUPTORES)

PALABRAS CLAVE: LAN conmutada, microsegmento, modelo M/M/1, puente, switch (interruptor), algoritmo de puente transparente, dirección MAC y algoritmo extendido libre (STA, por sus siglas para Spanning Free Algorithm).

15.2.1 Ventajas y desventajas de las LAN de medios compartidos

Cuando se construyen redes pequeñas constituidas de 10 a 30 nodos, el uso de las tecnologías estándar basadas en un medio compartido es una solución económica y eficaz. Esta eficacia es el resultado de las siguientes propiedades de la red:

- La **topología de red simple**, que permite que el número de nodos de la red se incremente con facilidad dentro de límites razonables.
- La **eliminación de pérdidas de tramas**, causadas por el sobreflujo del búfer en los dispositivos de comunicaciones. Este resultado se consigue debido a que una nueva trama no se transmite en la red hasta que la anterior es recibida. La lógica del medio compartido regula el flujo de las tramas al forzar a las estaciones que generan tramas con demasiada frecuencia para que difieran sus envíos. Tales estaciones deben esperar hasta que tengan acceso al medio. De este modo, los procedimientos de control de flujo se llevan a cabo de manera automática.
- La **simplicidad de protocolos**, la cual ha asegurado el bajo costo de los adaptadores, repetidores y concentradores de red y, en consecuencia, de la red en su totalidad.

No obstante, la declaración de que grandes redes que conectan cientos o miles de nodos no pueden ser creadas con base en un medio compartido simple también es verdadera. Esto es cierto incluso para tecnologías de tan alta velocidad como Gigabit Ethernet. Prácticamente todas las tecnologías limitan tanto la longitud máxima de la red como el número de nodos en un medio compartido. Por ejemplo, para todas las tecnologías de la familia Ethernet, este número está limitado a 1 024 nodos; para Token Ring, este número es de 260 nodos, y para FDDI es de 500 nodos. A pesar de ello, ésta no es la única razón para una limitación así.

> El problema principal con todas las redes basadas en un medio compartido simple es la falta del ancho de banda.

Una extensión cuantitativa de los procesos que tiene lugar en una LAN de medio compartido podrá obtenerse si se usan modelos de colas. Un modelo de esta naturaleza (el M/M/1) se estudió en el capítulo 7. De acuerdo con este modelo, el medio compartido corresponde al servidor y las tramas generadas por cada computadora de la red corresponden a solicitudes de servicio. La cola de las solicitudes de servicio se distribuye entre todas las computadoras de la red, donde las tramas esperan su turno para utilizar el medio.

El modelo M/M/1 no puede reflejar de manera adecuada muchas características específicas de una LAN de medio compartido, como las colisiones Ethernet. No obstante, es capaz de demostrar un patrón cualitativo de la dependencia entre los retardos de acceso al medio y el coeficiente de utilización del medio.

La figura 15.1 muestra curvas de dependencia obtenidas para Ethernet, Token Ring y FDDI, para lo cual se emplean técnicas de simulación.

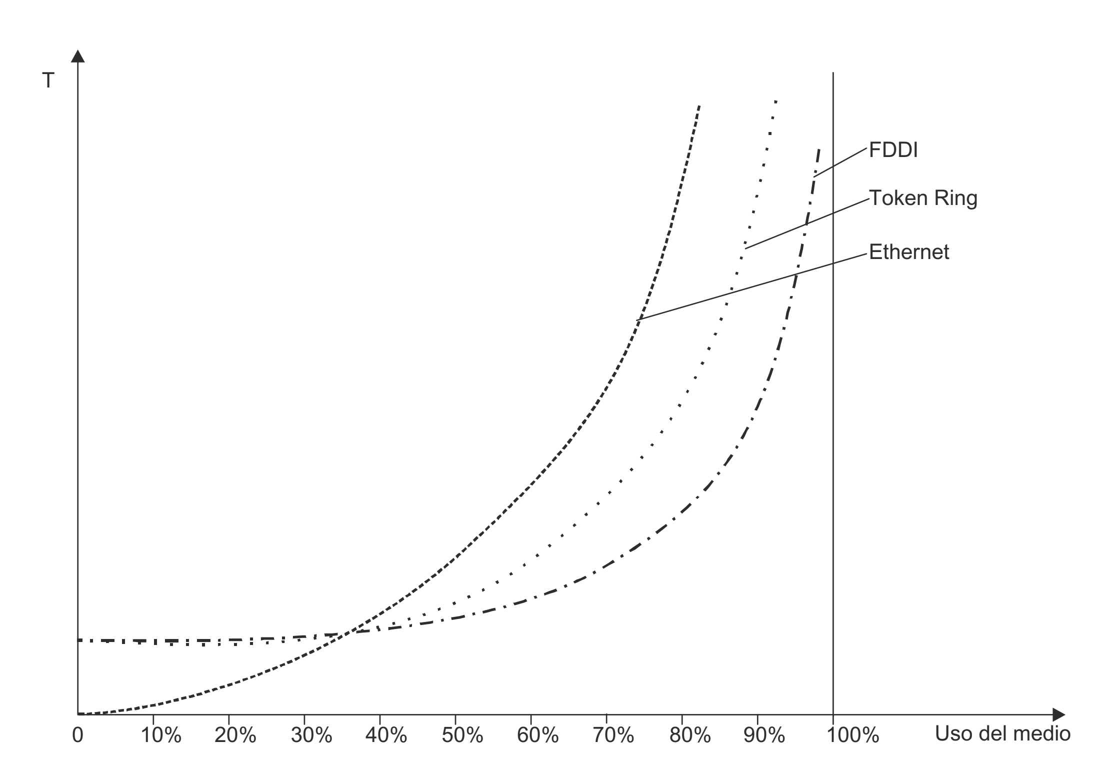


FIGURA 15.1 Retardos de acceso al medio para las tecnologías Ethernet, Token Ring y FDDI.

Como puede verse en esta ilustración, todas las tecnologías tienen un patrón cualitativamente similar de crecimiento exponencial del retardo contra la carga. En todos los casos, los retardos de acceso al medio crecen de manera exponencial con el incremento del uso del medio compartido. Sin embargo, difieren en un valor del umbral en el que ocurren cambios agudos en el comportamiento de la red, cuando la dependencia casi lineal se convierte en un crecimiento fuertemente exponencial. Para todas las tecnologías de la familia Ethernet, este valor es de 30 a 50% (debido al efecto de colisión); para Token Ring, este valor es de cerca de un 60% y para FDDI de 70 a 80%.

El número de nodos para el que el uso del medio compartido comienza a aproximarse al límite peligroso depende del tipo de aplicaciones que corran en los nodos de la red. Por ejemplo, antes se consideraba que 30 nodos era un número aceptable de nodos Ethernet en un segmento compartido. En la actualidad, si los nodos de la red ejecutan aplicaciones multimedia o intercambian grandes archivos de datos, este número puede ser de cinco a 10 nodos.

15.2.2 Ventajas de la estructuración de una red lógica

Es posible superar las limitaciones ocasionadas por la utilización de un medio compartido simple al dividir la red en varios medios compartidos y después conectar los segmentos separados de la red al usar dispositivos especiales de comunicaciones, como puentes, switches o enrutadores (figura 15.2).

Estos dispositivos transmiten las tramas de puerto en puerto con base en un análisis de la dirección de destino contenida en esas tramas. Los puentes y switches llevan a cabo la operación de la transmisión de la trama con apoyo en direcciones de capas de enlace de datos fijas (direcciones MAC) y los enrutadores utilizan direcciones jerárquicas de capa de red para este propósito. El funcionamiento de los enrutadores se estudiará con detalle en la parte IV. Por el momento, el interés se centrará en los puentes y los switches.

La estructuración lógica de la red se analizó brevemente en el capítulo 3. En esta sección, dicho problema se examinará con más detalle. La estructuración lógica de la red permite resolver varias tareas; las principales son la mejora del rendimiento, así como la flexibilidad, seguridad y manejabilidad de la red.

Mejora del rendimiento. Para ilustrar de mejor manera este efecto, el objetivo principal de la estructuración lógica, considérese la figura 15.3. Esta ilustración muestra dos segmentos Ethernet conectados por un puente. Entre esos segmentos hay varios repetidores. Antes que la red fuera segmentada, todo el tráfico generado por los nodos de la red compartía el mismo medio, por ejemplo: si en lugar de un dispositivo entre redes (puente), se hubiera instalado un repetidor. Esta red fue tomada en cuenta al determinar el coeficiente de utilización de la red. Si se designa la intensidad de promedio del tráfico que viaja desde el nodo i hasta el nodo j como C_{ij}, el tráfico total de la red tendrá que transmitir antes de la segmentación sería $C_\Sigma = \Sigma C_{ij}$ (considerando que la sumatoria se realice sobre todos los nodos).

Después de la segmentación, fue necesario tomar en cuenta el tráfico interno del segmento, es decir, las tramas que circulan entre los nodos dentro de un segmento simple y el tráfico entre segmentos que está dirigido desde un nodo de este segmento hacia el nodo de otro segmento, o que llega al nodo de este segmento desde el nodo perteneciente al otro segmento.

De lo anterior se infiere que la carga del segmento de, por ejemplo, el segmento S1 llega a ser igual a $C_{S1} + C_{S1\text{-}S2}$, donde C_{S1} es el tráfico interno del segmento S1 y $C_{S1\text{-}S2}$ es el tráfico

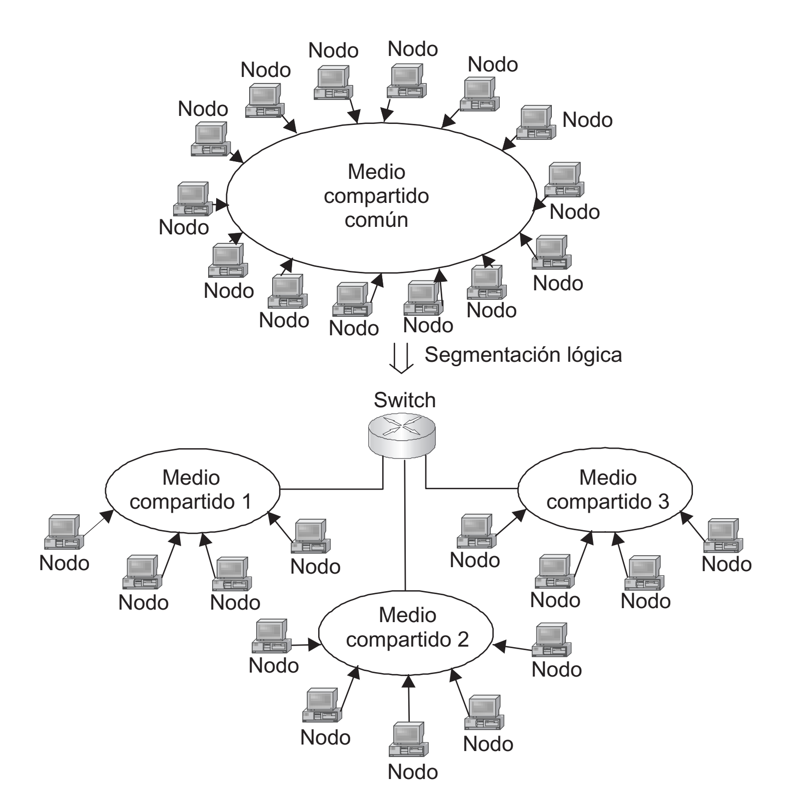


FIGURA 15.2 Estructura lógica de la red.

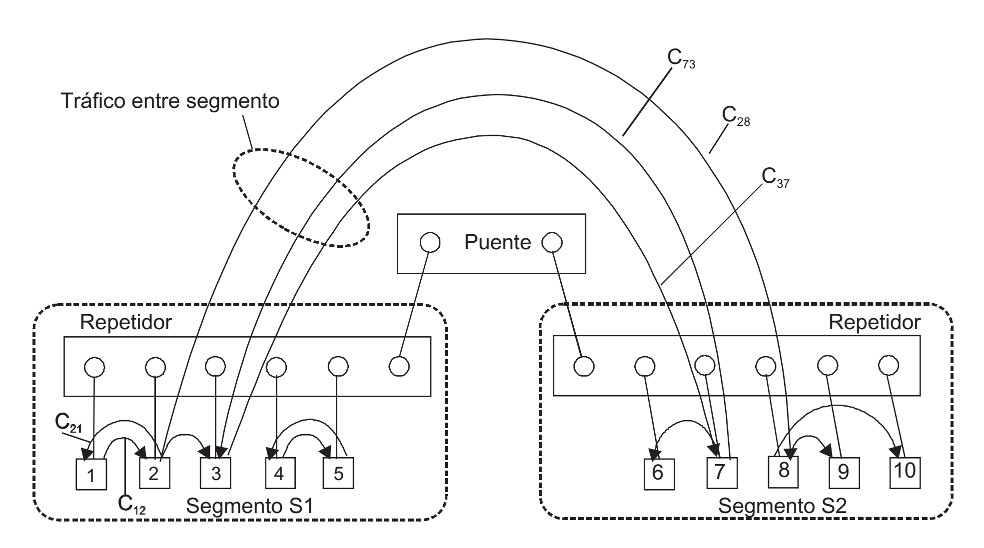


FIGURA 15.3 Cambio de la red después de la segmentación.

entre segmentos. Para ver que la carga sobre el segmento S1 llega a ser inferior a la carga de la red inicial, nótese que la carga total de la red antes de dividirla en segmentos puede escribirse de la forma siguiente: $C_{\Sigma} + C_{S1} + C_{S1\text{-}S2} + C_{S2}$. En consecuencia, la carga del S1 después de la segmentación llega a ser igual a $C_{\Sigma} - C_{S2}$, lo cual significa que ha disminuido por el valor del tráfico interno del segmento S2. Consideraciones similares pueden repetirse

para el segmento S2. De este modo, de acuerdo con las gráficas proporcionadas en la figura 15.1, los retardos en los segmentos han disminuido y el ancho de banda efectivo por nodo se ha incrementado.

Con anterioridad se mencionó que la segmentación de la red prácticamente reduce siempre la carga en nuevos segmentos. La palabra *prácticamente* toma en cuenta un evento tan extraño como aquel en el que una red se divide en segmentos de tal modo que el tráfico interno de cada segmento sea cero, lo cual significa que todo el tráfico ocurre entre segmentos. Para el ejemplo mostrado en la figura 15.3, esto significaría que todas las computadoras del segmento S1 intercambian datos sólo con computadoras pertenecientes al segmento S2, y viceversa.

En la práctica, en cualquier red es posible seleccionar un grupo de computadoras que pertenezcan a empleados que realicen algunas tareas comunes. Éstos pueden ser empleados pertenecientes al mismo grupo de trabajo, departamento u otra unidad estructural de la compañía. En la mayoría de los casos, necesitan tener acceso a los recursos de la red de su departamento y sólo rara vez requieren el acceso a recursos remotos.

En la década de 1980 existió una regla empírica que establecía que era posible dividir la red en segmentos para asegurar que 80% del tráfico total lo causarían intentos de acceso a recursos locales y sólo 20% sería de acceso a recursos remotos. Una regla así no siempre refleja la realidad; por el contrario, puede transformarse en la regla de 50-50% o incluso de 20-80%. Por ejemplo, éste es el caso cuando la mayoría de los intentos para tener acceso a los recursos tiene como finalidad conseguir el acceso a Internet o a los recursos concentrados en los servidores de la compañía. No obstante, siempre hay tráfico interno del segmento. Si no hay tal tráfico, la red está dividida de manera incorrecta en segmentos.

Las subredes mejoran la flexibilidad de la red. Cuando se construye una red como un conjunto de segmentos (subredes), cada subred puede adaptarse de acuerdo con los requerimientos específicos de cierto grupo de trabajo o departamento. Por ejemplo, una subred puede utilizar la tecnología Ethernet y el sistema operativo UNIX, mientras que otra subred puede basarse en la tecnología Token Ring y ejecutar OS-400, de acuerdo con los requerimientos de un departamento específico o de las aplicaciones existentes. Los usuarios de ambas subredes podrán intercambiar datos si utilizan puentes o switches. El proceso de dividir la red en segmentos lógicos puede considerarse desde el punto de vista opuesto: el proceso de crear una gran red mediante la interconexión de las subredes existentes.

Las subredes fortalecen la seguridad de los datos. Al instalar varios filtros lógicos en puentes o switches, es posible controlar el acceso del usuario a los recursos en otros segmentos. Nótese que los repetidores no proporcionan esta capacidad.

Las subredes simplifican la administración de la red. La simplificación de la administración de la red es un efecto colateral de la reducción del tráfico y el mejoramiento de la seguridad de los datos. Los problemas suelen localizarse dentro de un segmento. Los segmentos forman dominios lógicos de administración de la red.

Como ya se mencionó, una red podrá dividirse en segmentos lógicos si se utilizan dos tipos de dispositivos: puentes y/o switches. Poco después de la llegada de los switches a principios de la década de 1990, los departamentos de mercadotecnia de las compañías que fabricaban estos nuevos dispositivos intentaron crear la falsa impresión de que el puente y el switch son dispositivos diferentes.

A pesar de ello, el puente y el switch tienen tanto en común que a nivel funcional parecen gemelos. La diferencia principal entre ellos es que un puente procesa tramas de manera secuencial, mientras que un switch efectúa la misma operación en paralelo.

Ambos dispositivos envían tramas con base en el mismo algoritmo: el **algoritmo de puente transparente** descrito en el estándar IEEE 802.1D.

Este estándar, diseñado mucho antes de que apareciera el primer switch, describía la operación de un **puente**. Por lo tanto, es natural que el término **puente** se haya mantenido en su nombre. Cuando aparecieron los primeros modelos de switches, surgió algo de confusión debido a que los switches funcionaban con base en el algoritmo de emisión de tramas descrito en el estándar IEEE 802.1D. Este algoritmo funciona por medio de puentes durante alrededor de 10 años. Aunque los puentes para los que el algoritmo fue diseñado están casi fuera de uso en la actualidad y son dispositivos de comunicación obsoletos, los estándares describen de modo tradicional el funcionamiento del switch, para lo cual utilizan el término **puente**; no obstante, no hay que ser tan conservador. Cuando se describan los algoritmos del estándar IEEE 802.1D en la siguiente sección se utilizará el término **switch**, excepto cuando se menciona el nombre oficial de un estándar o cuando es necesario destacar la diferencia entre los dos tipos de dispositivos.

15.2.3 Algoritmo de puente transparente del estándar IEEE 802.1D

La palabra ***transparente*** en el nombre del algoritmo de puente transparente refleja el hecho de que los puentes y los switches en su funcionamiento no toman en cuenta los adaptadores de red de los nodos, concentradores y repetidores terminales. Por otra parte, los dispositivos enumerados con antelación también funcionan sin advertir la presencia de puentes y switches.

El algoritmo de puente o switch transparente no depende de la tecnología LAN utilizada en la LAN donde se instala el puente. Por ende, los puentes o switches transparentes de Ethernet funcionan de la misma manera que los puentes o switches transparentes FDDI o Token Ring.

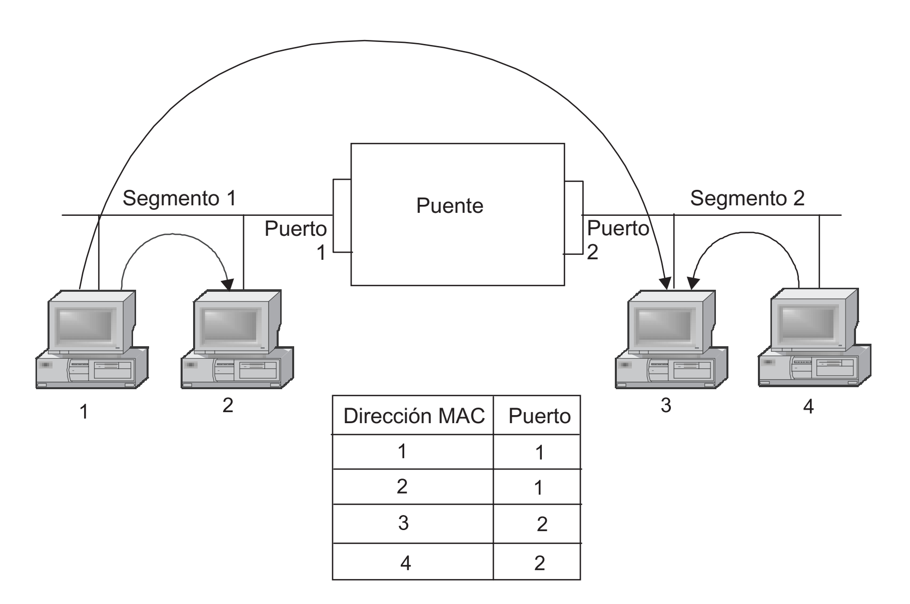
El switch crea su tabla de direcciones al examinar de manera pasiva el tráfico que circula en los segmentos conectados a sus puertos. Además, toma en cuenta las direcciones iniciales o fuente de los datos que llegan a sus puertos de switch y determina el segmentos de red al cual pertenece un nodo fuente específico con base en la dirección fuente conducida por una trama enviada por ese nodo.

NOTA *Cada puerto del switch funciona como un nodo terminal de su segmento con una excepción: que el puerto del switch no tenga una dirección MAC propia. Los puertos de switch no necesitan direcciones debido a que funcionan en el modo promiscuo de captura de trama. En este modo, todas las tramas que llegan al puerto se cargan en la memoria temporal del búfer, sin tener en cuenta sus direcciones de destino. Cuando funciona en el mundo promiscuo, el switch "escudriña" todo el tráfico circulante en los segmentos conectados a él y utiliza las tramas que pasan a través de él para aprender la estructura de la red.*

Considérese cómo el switch genera y utiliza de manera automática la tabla de dirección en el ejemplo de una red simple mostrado en la figura 15.4.

El switch conecta dos segmentos red. El segmento 1 consta de computadoras conectadas por un elemento simple de cable coaxial al puerto 1 del switch. El segmento 2 se compone de computadoras conectadas al puerto 2 del switch en las que emplea otra sección de cable coaxial.

En un principio, el switch no conoce las direcciones MAC de las computadoras conectadas a cada uno de sus puertos. En esta situación, el switch sólo transmite cualquier trama



Dirección MAC	Puerto
1	1
2	1
3	2
4	2

FIGURA 15.4 Principio de operación de un switch o puente transparente.

capturada y almacenada a todos sus puertos, con excepción del puerto desde el que se recibió dicha trama. En este ejemplo, el switch tiene sólo dos puertos; por lo tanto, transmite las tramas desde el puerto 1 hasta el 2 y viceversa. La diferencia entre un switch que funciona en este modo y un repetidor es que el switch transmite la trama al almacenar temporalmente todos los datos de la misma antes que la trama se transmita en lugar de la transmisión bit por bit. El almacenamiento temporal rompe la lógica de operación de todos los segmentos como un medio compartido simple. Cuando el switch se dispone a transmitir la trama de segmento a segmento (por ejemplo del segmento 1 al segmento 2) intenta de nuevo tener acceso al segmento 2 de manera similar a un nodo terminal en el que usa un algoritmo de acceso al medio específico (en este caso, CSMA/CD).

Durante la transmisión de la trama a todos los puertos, el switch aprende la dirección fuente inicial de la trama e introduce el registro de que pertenece a un segmento específico en la *tabla de dirección* del switch, también conocida como *tabla de filtrado* o *tabla de enrutamiento.* Por ejemplo, una vez que ha recibido una trama desde la computadora 1 hasta su puerto 1, el switch incluye el primer registro en su tabla de dirección:

MAC address1 – port 1

Este registro significa que la computadora con la dirección 1 de MAC, **MAC address1**, pertenece al segmento conectado al puerto 1, **port 1**, del switch. Si las cuatro computadoras de esta red se encuentran activas e intercambian tramas entre sí, el switch pronto construirá una tabla de dirección completa de esta red, compuesta de cuatro registros, un registro por nodo terminal (figura 15.4).

En cualquier momento en que llega una trama al puerto del switch, éste intenta usarlo al comparar las direcciones de destino de todas las tramas que llegan a esta dirección y verificar si coinciden. Ahora continuamos el estudio del funcionamiento del switch en el ejemplo mostrado en la figura 15.4.

1. Una vez recibida una trama enviada desde la computadora 1 hasta la 3, el switch examinaría la tabla de dirección para hallar la dirección que coincide con la dirección del destino especificada en la trama: **MAC address3**. Existe un registro así en la tabla.

2. El switch lleva a cabo la segunda etapa del análisis de la tabla. En esta etapa, el switch verifica si las computadoras con la dirección fuente (**MAC address1**) y la dirección destino (**MAC address3**) se localizan en el mismo segmento; en otras palabras, si se conectan al mismo puerto. En este ejemplo, las computadoras 1 y 3 están localizadas en segmentos diferentes; por lo tanto, el switch realiza la operación conocida como *direccionamiento de trama:* transmite la trama a otro puerto, en cuanto ha obtenido el acceso a otro segmento con anterioridad.
3. Si el switch encuentra que las computadoras con las direcciones especificadas de fuente y destino pertenecen al mismo segmento, simplemente eliminará la trama de su memoria temporal o búfer. Esta operación se conoce como *filtrado*.
4. Si la dirección de destino es **desconocida para** (**no aprendida por**) **el switch**, lo cual significa que no se encuentra la tabla de dirección, el switch transmitirá la trama a todos sus puertos, excepto al puerto fuente o de inicio, de manera semejante a la etapa inicial del proceso de aprendizaje.

El proceso de aprendizaje del switch nunca se detiene y ocurre en paralelo con el filtrado y el direccionamiento de tramas. El switch rastrea de manera constante las direcciones de inicio o fuente de las tramas que se almacenan para adaptarse de manera automática a los cambios que pueden ocurrir en la red, como el traslado de las computadoras de segmento a segmento, la eliminación de computadoras y la inclusión de nuevas computadoras.

Las entradas de la tabla de dirección pueden ser *dinámicas* (creadas por el switch en el proceso de autoaprendizaje) o *estáticas* (creadas en forma manual por un administrador de la red). Las **entradas estáticas** no tienen tiempo de expiración, lo cual permite que un administrador influya en el funcionamiento de una computadora específica; por ejemplo, al limitar la transmisión de tramas que tengan direcciones fuente o de inicio específicas de segmento a segmento.

Las **entradas dinámicas** tienen un tiempo de expiración; cuando se actualiza una entrada existente en la tabla de dirección o cuando se crea una nueva entrada, se asocia una marca de tiempo con ella. Después de finalizar el tiempo predefinido, el registro se marcará como inválido si durante ese tiempo el switch no ha recibido una trama sencilla con esa dirección en el campo de direcciones fuente: ésta permite relacionar eventos de manera automática cuando las computadoras se mueven de segmento a segmento. Si una computadora se desconecta de su segmento previo, la entrada en la tabla de dirección que especifica que esta computadora pertenece a ese segmento se eliminará de la tabla de dirección después de un tiempo. Luego de que esta computadora se conecte a otro segmento, sus tramas llegarán al búfer del switch a través de otro puerto y se incluirá un nuevo registro en la tabla de dirección correspondiente a nuevo estado de la red.

Las tramas con direcciones MAC de difusión y las que tienen direcciones de destino no aprendidas se pasan mediante el switch a todos sus puertos. Este modo de propagación de tramas se conoce como tormenta *broadcast* (*inundación*). La presencia de switches en la red no evita la propagación de tramas de difusión por todos los segmentos de la red, pero preserva su transparencia. A pesar de ello, esta característica será una ventaja sólo si la dirección de difusión se ha creado por el nodo que funciona correctamente.

No obstante, con frecuencia pueden surgir situaciones en las que, como resultado de fallas o un mal funcionamiento del software, el protocolo de capa superior o el adaptador de la red comiencen a funcionar de manera incorrecta: generan de forma constante tramas de difusión durante un largo tiempo. En este caso, el switch transmite dichas tramas a todos los segmentos e inunda de esta manera la red con tráfico inválido. Una situación de esta naturaleza se conoce como *tormenta de difusión.*

Por desgracia, los switches no son capaces de proteger las redes contra las tormentas de difusión, por lo menos en forma predeterminada, en contraste con los enrutadores (esta propiedad de los enrutadores se estudiará en la parte IV). Lo más que puede hacer un administrador para evitar una tormenta de difusión al usar un switch es especificar para cada nodo la intensidad máxima de generación de tramas con una dirección de difusión. En este caso, es necesario conocer con precisión cuál intensidad es normal y cuál indica una situación errónea. Cuando se cambian los protocolos, la situación en la red puede modificarse. En particular, la situación que ayer se consideraba errónea puede probar hoy ser bastante normal.

La figura 15.5 muestra una estructura típica de un switch. Las funciones de acceso al medio cuando se reciben y transmiten tramas se llevan a cabo mediante circuitos MAC, que son similares a los correspondientes de un adaptador de red.

El protocolo que pone en marcha el algoritmo de switch reside entre las capas MAC y LLC (figura 15.6).

La figura 15.7 muestra una copia de la pantalla de la terminal con la tabla de dirección del módulo de switch local. La terminal está conectada al puerto de la consola y la información exhibida en su pantalla es generada por la unidad de control del switch.

En la tabla de dirección (tabla de direccionamiento) que se exhibe en la pantalla puede verse que la red comprende dos segmentos: LAN A y LAN B. En el segmento de la LAN A existen al menos tres estaciones y en el segmento de la LAN B hay dos. Las cuatro direcciones marcadas con asteriscos son direcciones estáticas (es decir, están asignadas en forma manual por un administrador de la red). La dirección marcada con el signo de suma es una dirección dinámica con el tiempo expirado.

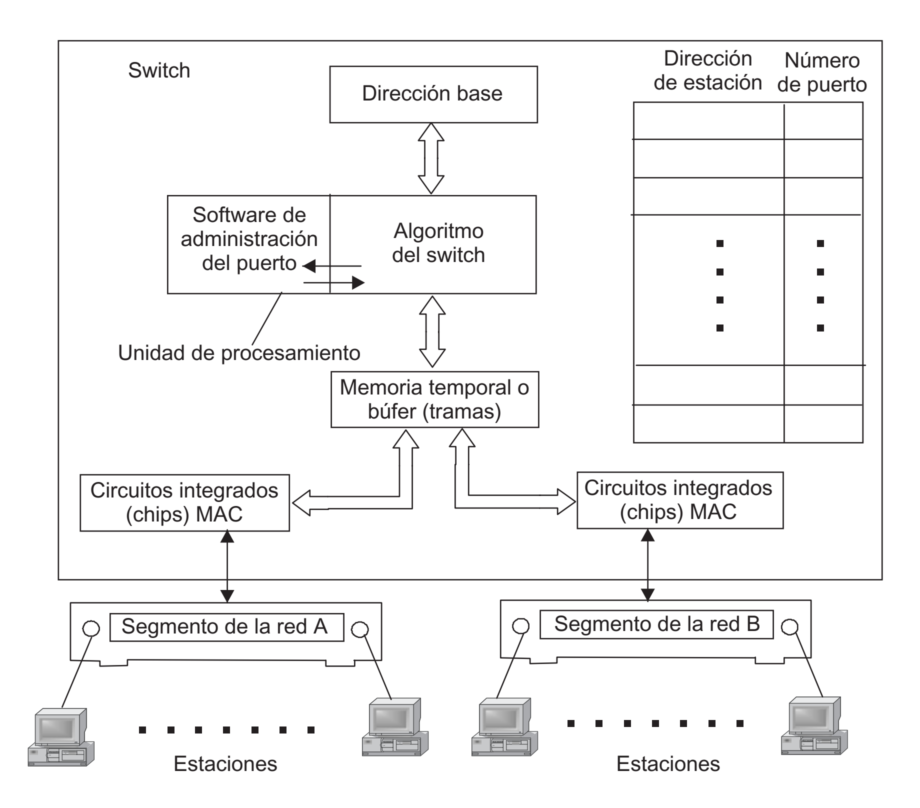


FIGURA 15.5 Estructura de un switch.

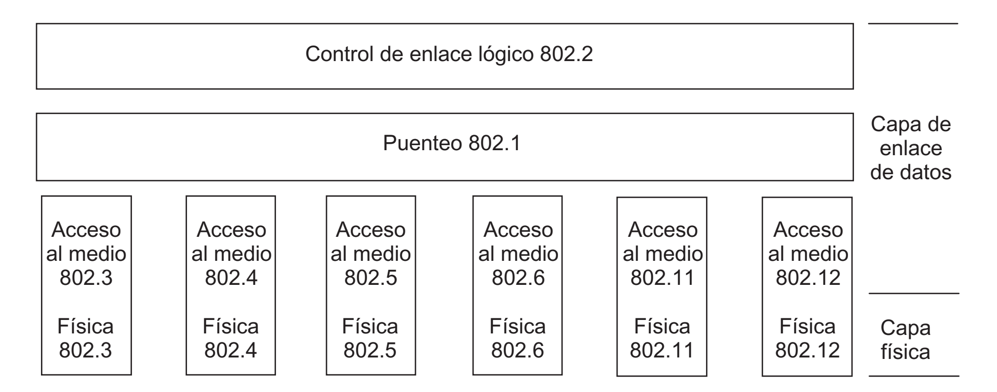


FIGURA 15.6 Ubicación del protocolo de switch en la pila de protocolo.

Página 1 de 1

Dirección	Dispn	Dirección	Dispn	Dirección	Dispn
00608CB17E58	LAN B	0000810298D6	LAN A	02070188ACA	LAN A
00008101C4DF	LAN B	+000081016A52	LAN A	*010081000100	Flood (Inundación)
*010081000101	Discard (Descartar)	*0180C2000000	Discard (Descartar)	*000081FFD166	Flood (Inundación)

Estado de dirección: TTL expirado

Salir Página siguiente Página anterior Editar tabla Buscar elemento Ir a página

+ Olvidado *Estático Entradas totales = 9 Entradas estáticas = 4

Use las teclas del cursor para elegir la opción. Pulse <Intro> para seleccionar.
Presione <CTRL> <P> para regresar al Menú Principal

FIGURA 15.7 Tabla de dirección de un switch.

La tabla tiene la columna rotulada como *Dispn*: disposición. Los datos en esta columna informan al switch que la operación debería llevarse a cabo sobre una trama que tiene la dirección de destino especificada. Cuando la tabla se crea automáticamente, este campo suele contener una designación convencional del puerto de destino. No obstante, cuando la dirección se especifica de modo manual, es posible especificar la operación no estándar del procesamiento de trama en este campo. Por ejemplo, la operación *Flood* (*inundación*) hace que el switch distribuya las tramas en modo de difusión, aun cuando su dirección de destino no sea una de difusión. La operación *Discard* (*descartar*) instruye al switch para que descarte la trama con una dirección, en vez entregarla al puerto de destino.

Las operaciones especificadas en la columna *Dispn* definen condiciones específicas de filtrado de trama y complementan las condiciones estándar de su propagación. Tales condiciones en general se conocen como *filtros definidos por el usuario.* Esto se estudiará más adelante en la sección "Filtrado del tráfico".

15.2.4 Limitaciones topológicas de la LAN conmutada

Una seria limitación de las capacidades funcionales de estos dispositivos de comunicaciones es la imposibilidad de soportar configuraciones en ciclo cerrado (loop) de la red.

Considérese esta limitación en el ejemplo de la red que se muestra en la figura 15.8.

En este ejemplo, dos segmentos de Internet están conectados en paralelo mediante los switches de tal manera que se forma un ciclo o loop activo. Supongamos que una nueva estación con una dirección MAC de 123 se conecta por primera vez a esta red e inicia su operación. Por lo regular, el arranque de cualquier sistema operativo está acompañado por la transmisión de tramas de difusión en las cuales la estación informa a otras computadoras que se encuentra en la red y simultáneamente busca los servidores de la red.

En la primera etapa, la estación envía la primera trama con la dirección de destino de difusión y la dirección fuente 123 en el segmento local. Esta trama llega a los switches 1 y 2. En ambos switches, la nueva dirección fuente, 123, se introduce en la tabla de dirección con la marca y especifica que pertenece al segmento 1. Esto significa que se crea una nueva entrada de la tabla de dirección, que se muestra como sigue:

Dirección MAC	**Puerto**
123	1

Como la dirección de destino es una dirección de difusión, cada switch debe transmitir la trama hacia el segmento 2. Esta transmisión sale en turnos de acuerdo con el método de acceso aleatorio de la tecnología Internet. Supóngase que el switch 1 fue el primero en obtener el acceso al segmento 2 (etapa 2 en la figura 15.8). Cuando la trama llega al segmento 2, el switch 2 la recibe, la carga en su búfer y la procesa. El switch 2 advierte que la dirección 123 ya se encuentra en su tabla de dirección, pero la trama que acaba de llegar es más reciente y establece que la dirección 123 pertenece al segmento 2 en lugar de al segmento 1. Por lo tanto, el switch 2 corrige el contenido de su tabla de dirección y crea una entrada nueva que especifica que la dirección 123 pertenece al segmento 2:

Dirección MAC	**Puerto**
123	2

El switch 1 procede de manera semejante cuando el switch 2 transmite su copia de la trama hacia el segmento 2.

Así, la presencia del ciclo o loop produce los resultados siguientes:

- La "formación" ("spawning") de tramas (por ejemplo, la aparición de varias copias de la misma trama). En este caso, existen dos copias; si los segmentos estuvieran conectados por tres switches, habría tres copias, y así sucesivamente.
- La circulación indefinida de ambas copias de la trama en direcciones inversas a lo largo del ciclo cerrado o loop, lo que implica la inundación de la red con tráfico inútil.
- La reconstrucción constante de tabla de dirección de los switches, pues la trama con la dirección fuente 123 aparecerá de manera constante en un puerto y luego en otro.

Para eliminar esos efectos indeseables, los switches deben ser utilizados con el fin de suprimir los ciclos cerrados entre segmentos lógicos. Esto significa que los switches permiten construir únicamente estructuras de árbol que garanticen la presencia de sólo una ruta entre dos segmentos cualesquiera. Las tramas desde cada estación siempre arribarán al switch

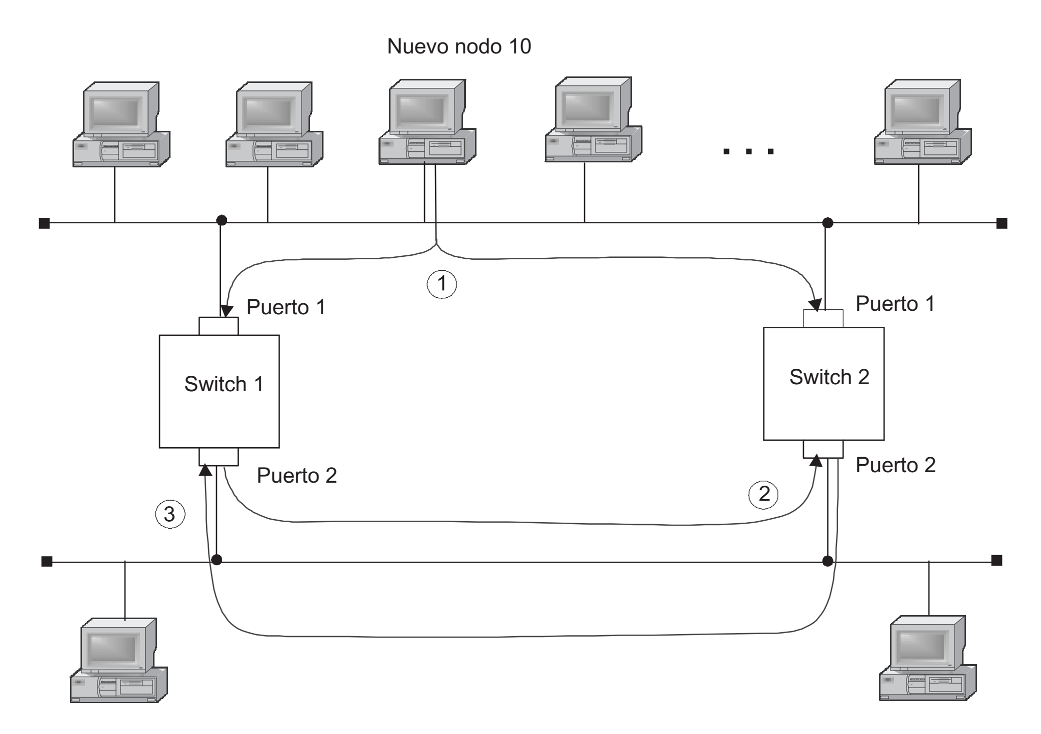


FIGURA 15.8 Influencia de las rutas cerradas sobre la operación de un switch.

desde el mismo puerto, y el switch será capaz de elegir de manera correcta una ruta racional dentro de la red. Ésta es una topología arbórea de red.

En redes pequeñas, es comparativamente fácil garantizar la existencia de una trayectoria posible entre dos segmentos. No obstante, a medida que crece el número de conexiones, la probabilidad de crear de manera no intencional ciclos cerrados también es más grande.

Asimismo, para mejorar la confiabilidad de la red es deseable tener enlaces de reserva entre switches, los cuales no participan en la transmisión de la trama cuando los enlaces principales funcionan de modo normal, pero restablecerán la conectividad mediante la creación de una nueva configuración de trabajo sin ciclos cerrados si falla uno de los enlaces principales.

De lo anterior se infiere que en redes complejas se crean enlaces redundantes entre los segmentos. A su vez, estos enlaces generan ciclos o loops. Para eliminar los ciclos activos, se deben asegurar algunos puertos de los switches. La manera más simple de resolver este problema es la configuración manual; a pesar de ello, existen algoritmos que permiten que este problema se resuelva de manera automática. El más conocido de ellos es el **algoritmo de árbol extendido** (**STA**), que se estudiará con detalle en el capítulo 16.

15.3 SWITCHES (INTERRUPTORES)

PALABRAS CLAVE: switch o interruptor, fuente, algoritmo de árbol extendido (STA, Spanning Tree Algorithm), matriz de conmutación, filtrado del tráfico y Kalpana.

15.3.1 Características específicas de los switches

Con los cambios radicales en la evolución de la red que tuvieron lugar a finales de la década de 1980 y principios de la de 1990, que causaron el arribo de protocolos rápidos, las PC

de alto rendimiento e información multimedia, además de la división de las redes en gran número de segmentos, los **puentes** clásicos dejaron de realizar sus tareas adecuadamente. El servicio de flujos de tramas entre varios puertos en los que se utilizaba una sola unidad de procesamiento requería un incremento significativo en la velocidad de operación del procesador, lo cual implicaba una solución costosa.

Se encontró una solución más eficaz, que produjo el desarrollo de los switches: para atender un flujo que llega a cada puerto, el dispositivo fue equipado con un procesador por separado que implementaba el algoritmo de puente. Por su naturaleza, el switch es un puente multiprocesador, capaz de direccionar tramas de manera simultánea entre todos los pares de sus puertos. No obstante, en contraste con las computadoras, las cuales no cambian su nombre después de haber agregado nuevos procesadores sino que simplemente se convierten en "configuraciones de multiprocesador", la situación con los puentes multiprocesadores era diferente; llegaron a conocerse como switches. Este cambio del nombre del dispositivo fue promovido por el método de organizar las conexiones entre los procesadores individuales dentro de un switch: estaban conectados mediante una matriz de conmutación, similar a las matrices de computadoras multiprocesador que conectaban los procesadores a la memoria.

En forma gradual, los switches han trasladado los puentes clásicos del procesador simple fuera de las LAN. La principal razón para esto fue el alto rendimiento asegurado por los switches al transmitir tramas entre segmentos de la red. En contraste con los puentes que tenían una operación de red aún lenta, los switches siempre están equipados con procesadores de puerto capaces de transmitir tramas a la velocidad máxima permitida por un protocolo. Al agregar la capacidad de transmitir las tramas entre puertos en paralelo, se ha hecho el rendimiento del switch decenas de veces superior al de los puentes. Este factor ha definido las perspectivas de los puentes y los switches.

Los switches pueden transmitir millones de tramas por segundo; los puentes por lo regular procesan de 3 000 a 5 000 tramas por segundo.

Durante un tiempo desde que existen, sin la competencia de los puentes, los switches han adoptado muchas funciones adicionales que aparecen como un resultado natural de la evolución de las tecnologías de red. La lista de tales funciones incluye soporte para LAN virtuales (VLAN), prioridad del tráfico y el uso del puerto troncal predeterminado.

La tecnología de los segmentos de Internet conmutados se sugirió primero por una compañía muy pequeña (Kalpana) en 1990 en respuesta a las necesidades de crecimiento al aumentar el ancho de banda de los enlaces que conectaban a servidores de alto rendimiento con los segmentos que contenían estaciones de trabajo.

Si el puerto de salida se encuentra disponible en la recepción de tramas, el retardo entre la recepción del primer byte y la llegada del mismo byte al puerto de salida es de sólo 40 μseg para el switch Kalpana. Éste es un valor bastante más bajo que el retardo de la trama que se transmite por medio de un puente.

El diseño estructural del switch o interruptor EtherSwitch sugerido por Kalpana se muestra en la figura 15.9.

Cada uno de los ocho puertos 10Base-T es servido por un solo **procesador de paquete Ethernet** (**EPP, Ethernet Packet Processor**). Aparte de éstos, el switch tiene una unidad de sistema que coordina el funcionamiento de todas las EPP. La unidad de sistema soporta la tabla de dirección común del switch. La matriz de conmutación se utiliza para transmitir las tramas entre los puertos, funciona de acuerdo con el principio de conmutación del circuito y conecta los puertos del switch. Para ocho puertos, tal matriz puede asegurar ocho canales

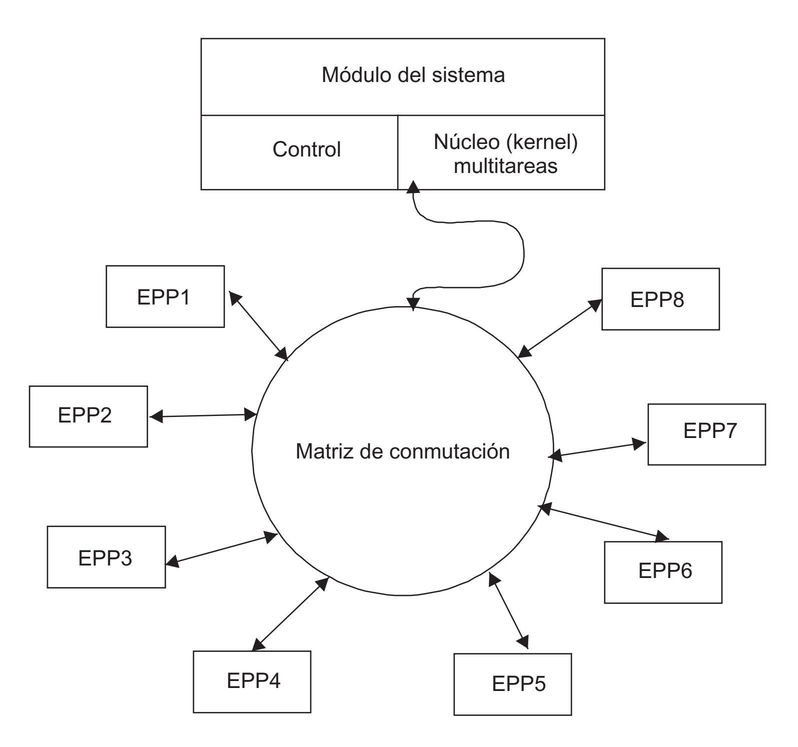


FIGURA 15.9 Diseño estructural del switch EtherSwitch sugerido por Kalpana.

internos simultáneos cuando se utiliza el modo de operación half-dúplex y 16 canales en el modo full-dúplex cuando el transmisor y el receptor funcionan de manera independiente.

Cuando llega una trama a uno de los puertos, el EPP almacena temporalmente los diversos primeros bytes de la trama para leer la dirección de destino. Después de recibir la dirección de destino, el procesador toma de manera inmediata una decisión acerca de la transmisión del paquete, sin tener que esperar la llegada de los bytes restantes de la trama. Para este propósito, observa su propio caché de la tabla de dirección. Si ahí encuentra coincidencia con la dirección necesaria, el EPP se dirigirá al módulo del sistema que funciona en el modo multitareas, atendiendo las solicitudes de todos los EPP en paralelo. El módulo del sistema revisa la tabla de dirección común y devuelve la entrada requerida hacia el procesador. El EPP almacena esta entrada en su caché para uso futuro.

- Si la dirección de destino se ha hallado en la tabla de dirección y debe filtrarse la trama recién llegada, el procesador simplemente tendrá los bytes de la trama que se cargan en el búfer o memoria temporal, lo limpiará y esperará a que llegue una nueva trama.
- Si la dirección de destino se ha encontrado en la tabla de dirección y la trama recién llegada debe transmitirse a otro puerto, el procesador se dirigirá a la matriz de conmutación mientras continúe cargando los bytes de la trama en el búfer e intentará establecer la trayectoria que conecta su puerto hacia el puerto a través del cual pasa la trayectoria hacia la dirección de destino. La matriz de conmutación puede hacer esto solamente cuando el puerto de la dirección de destino se encuentra libre, lo cual significa que en ese momento no se encuentra conectado a otro puerto.
- Si el puerto está ocupado, la matriz rechazará la solicitud para conexión, como ocurre con cualquier dispositivo basado en conmutación de circuitos. En este caso, la trama se almacena completamente en el búfer por el procesador del puerto de entrada, después

de lo cual el procesador espera hasta que el puerto de salida se libere y la matriz de conmutación cree la trayectoria requerida.

- Después de establecer la trayectoria requerida, los bytes de la trama almacenados en el búfer se dirigen a ella y el procesador del puerto de salida lo recibe. En cuanto el procesador del puerto de salida obtiene el acceso al segmento Ethernet conectado a él (mediante el uso del algoritmo CSMA/CD), los bytes de la trama comienzan a ser transmitidos de inmediato en la red. El procesador del puerto de entrada almacena constantemente varios bytes de la trama que se recibe en su búfer, lo que lo capacita para transmitir y recibir de manera independiente y asincrónica bytes de la trama (figura 15.10).

Este método de transmisión de trama sin lograr su almacenamiento completo llegó a conocerse como *conmutación al vuelo* o *mediante corte*. Principalmente, tal método consiste en el procesamiento canalizado de tramas en el que varias etapas de su transmisión se efectúan en paralelo. Las etapas son las siguientes:

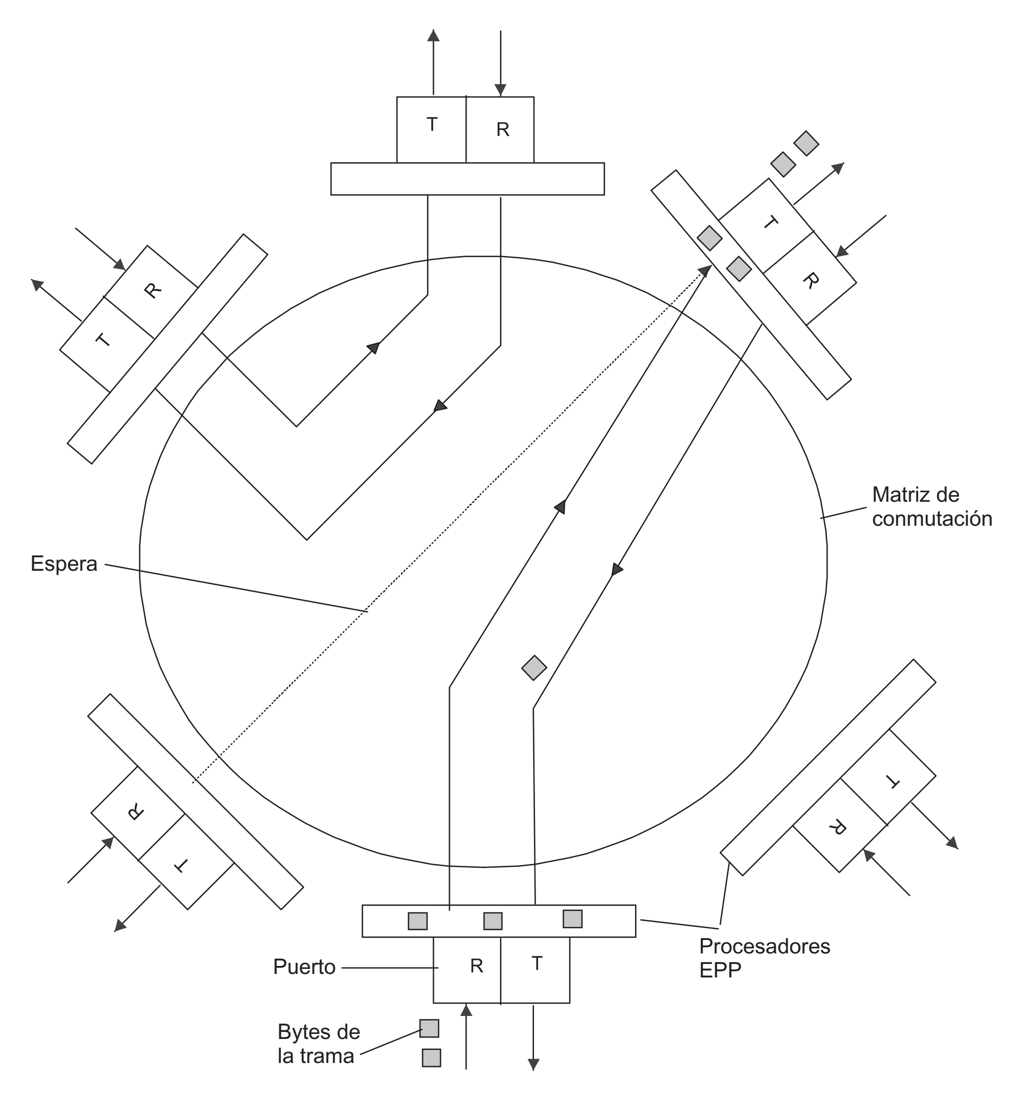


FIGURA 15.10 Transmisión de trama en la que se utiliza la matriz de conmutación.

1. Recepción de los primeros bytes de la trama por el procesador del puerto de entrada, incluidos los bytes que contienen la dirección de destino.
2. Búsqueda de la dirección de destino en la tabla de dirección del switch, ya sea en el caché EPP o en la tabla común del módulo del sistema.
3. Conmutación de la matriz.
4. Recepción de los bytes restantes de la trama por el procesador del puerto de entrada.
5. Recepción de los bytes de la trama (incluidos los primeros) por el procesador del puerto de salida a través de la matriz de conmutación.
6. Acceso del medio por el procesador del puerto de salida.
7. Transmisión de los bytes de la trama por el procesador del puerto de salida hacia la red.

La figura 15.11 ilustra dos modos del procesamiento de tramas: procesamiento canalizado de la trama en el cual varias etapas de su transmisión se realizan en paralelo, y procesamiento normal con almacenamiento temporal completo y ejecución secuencial de todas las etapas (nótese que las etapas 2 y 3 no pueden llevarse a cabo en paralelo, pues sin conocer el número del puerto de salida, la operación de conmutación de la matriz no tiene sentido).

Como puede verse en la ilustración, en comparación con el modo de almacenamiento temporal completo, la ganancia en tiempo asegurada mediante la canalización parece bastante impresionante.

A pesar de ello, el elemento principal que permite incrementar el rendimiento de la red al utilizar switches es el procesamiento paralelo de varias tramas.

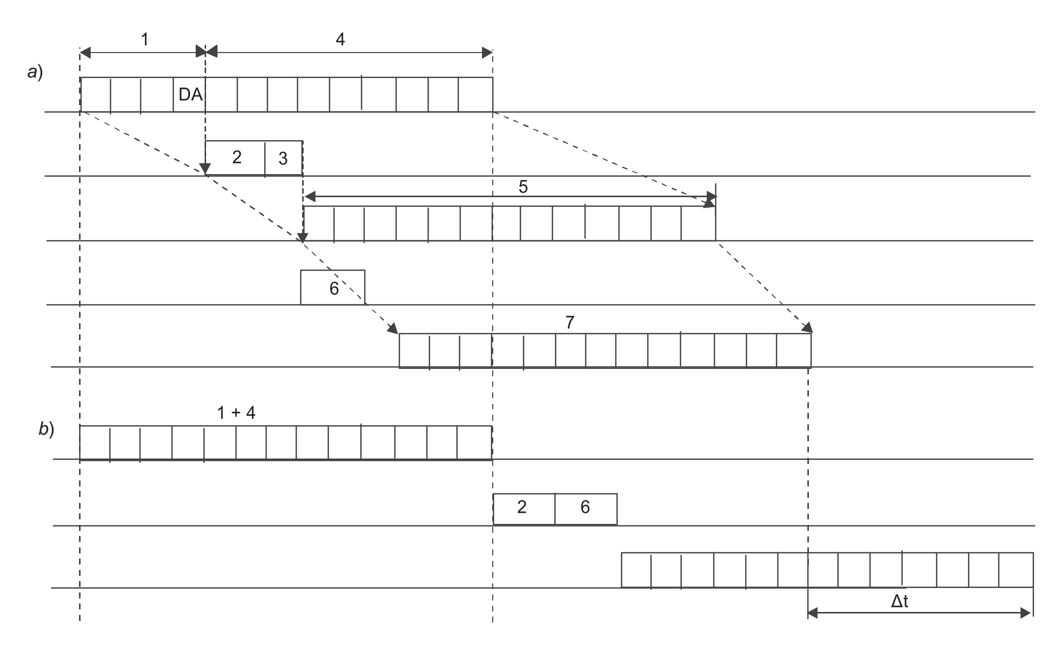


FIGURA 15.11 Tiempo ganado por el procesamiento de trama canalizado: procesamiento canalizado *a*) y procesamiento normal con almacenamiento temporal total *b*).

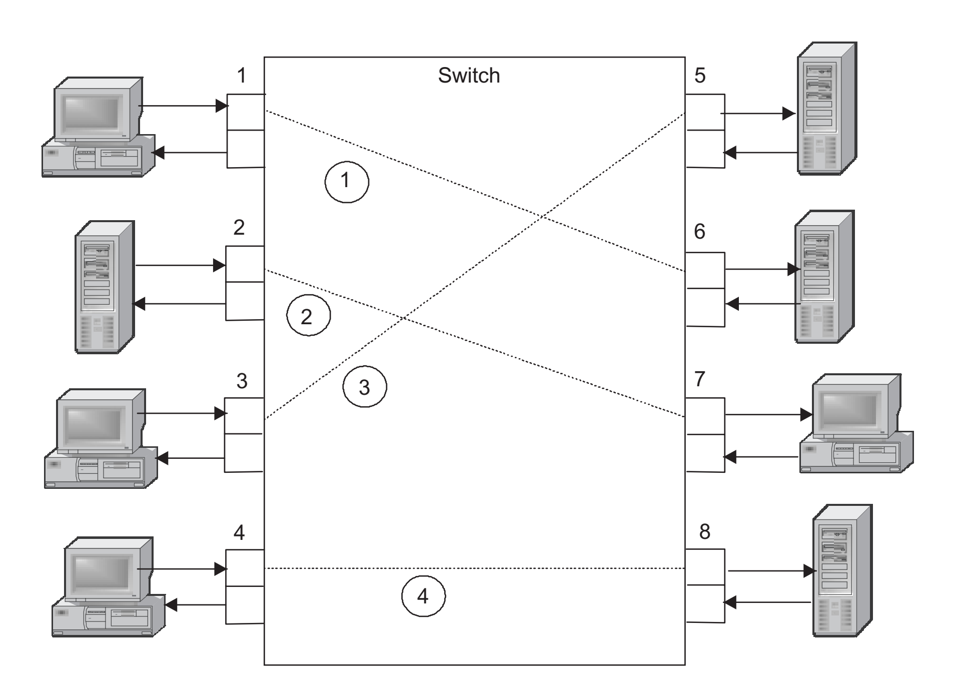


FIGURA 15.12 Transmisión en paralelo de tramas por medio de un switch (1-4 flujos de tramas entre computadoras).

Este efecto se ilustra en la figura 15.12, que muestra un rendimiento ideal cuando cuatro u ocho puertos transmiten datos a la velocidad máxima permitida por el protocolo Ethernet (10 Mbps) y estos datos se transmiten a los cuatro puertos restantes del switch sin conflicto alguno. La ausencia de conflictos significa que los flujos de datos entre los nodos de la red se distribuyen de tal manera que para cada puerto de entrada que recibe las tramas existe un puerto de salida disponible. Si el switch logra procesar el tráfico de entrada incluso a la intensidad máxima de llegadas de las tramas al puerto de entrada, el rendimiento total del switch en este ejemplo será de $4 \times 10 = 40$ Mbps. Al generalizar este ejemplo para N puertos, el rendimiento total del switch será $(N/2) \times 10$ Mbps. **En este caso, el switch proporciona a cada estación o segmento conectado a su puerto el ancho de banda asignado del protocolo.**

Como es natural, tal situación no siempre tiene lugar en la red. Por ejemplo, dos estaciones (suponiendo que sean las conectadas a los puertos 3 y 4) deben escribir datos simultáneamente al mismo servidor, que está conectado al puerto 8. En este caso, el switch no podrá asignar flujos de datos de 10 Mbps a cada estación porque el puerto 8 no puede transmitir los datos a la velocidad de 20 Mbps. Las tramas de ambas estaciones esperarán en las colas internas de los puertos 3 y 4 hasta que el puerto 8 de salida se encuentre disponible para transmitir la siguiente trama. Para una distribución así de flujos de datos, tendría sentido conectar el servidor al puerto más rápido, tal como Fast Ethernet.

15.3.2 Switches sin bloqueo

Un switch *sin bloqueo* es aquel que puede transmitir tramas a través de sus puertos a la velocidad a la cual llegan a ellos.

Como regla, cuando se habla acerca del modo estable sin bloqueo del funcionamiento del switch, se supone que el switch transmite las tramas a la misma velocidad a la cual éstas llegan durante un periodo arbitrario. Con el fin de asegurar este modo de operación, es necesario conseguir una distribución de flujos de tramas para el cual los puertos de salida puedan manipular con éxito la carga. Si se ha observado este requerimiento, el switch siempre podrá transmitir en promedio el mismo número de tramas a sus puertos de salida que la cantidad de tramas que llegan a sus puertos de entrada. Si el flujo de tramas entrante (para todos los puertos) en promedio excede el flujo de tramas de salida (también para todos los puertos), las tramas se acumularán en la memoria temporal del búfer del switch. Si la cantidad de memoria temporal disponible se sobrepasa (lo que se conoce como *sobreflujo del búfer*), el switch comenzará a descartar tramas.

Para asegurar el modo sin bloqueo de funcionamiento del switch, debe satisfacerse la siguiente condición simple:

$$C_k = (\Sigma C_{pi})/2 \qquad (15.1)$$

Aquí, C_K es el rendimiento del switch, mientras que C_{pi} es el rendimiento máximo del protocolo soportado por el i-ésimo puerto del switch.

El rendimiento total de los puertos toma en consideración cada paso de la trama dos veces, primero como una trama entrante y después como una trama saliente. Dado que en el modo de operación estable el tráfico entrante es igual al tráfico saliente, el rendimiento suficiente mínimo del switch para soportar el modo sin bloqueo de operación es la mitad del rendimiento total de sus puertos. Si el puerto funciona en el modo half-dúplex, por ejemplo, Ethernet de 10 Mbps, el rendimiento del puerto (C_{pi}) será de 10 Mbps; si funciona en el modo full-dúplex, su rendimiento será de 20 Mbps.

En ocasiones, los enunciados declaran que el switch asegura un *modo sin bloqueo instantáneo.* Esto significa que el switch puede recibir y procesar tramas desde todos sus puertos a la máxima velocidad asegurada por los protocolos soportados, ya sea que se satisfaga o no el equilibrio estable entre el tráfico entrante y el tráfico saliente. A decir verdad, algunas tramas se pueden procesar de manera incompleta: si el puerto de salida está ocupado, la trama se cargará dentro del búfer o memoria temporal del switch.

Para soportar un modo sin bloqueo e instantáneo de operación, el switch debe proporcionar un rendimiento total superior, que en este caso debe ser igual al rendimiento total de sus puertos:

$$C_k = \Sigma C_{pi} \qquad (15.2)$$

No es un accidente que el primer switch del LAN estuviera dirigido a la tecnología Ethernet. Aparte de la alta popularidad de Ethernet, había otra razón importante: esta tecnología es más vulnerable a un incremento del retardo debido a la necesidad de esperar para tener acceso al medio cuando el segmento se encuentra sobrecargado. Por ello, los segmentos Ethernet en redes grandes fueron los primeros candidatos que necesitaban eliminar los cuellos de botella de la red. Los switches de Kalpana y más adelante los de otros fabricantes proporcionaron los medios para resolver este problema.

Algunas compañías comenzaron a desarrollar la tecnología de conmutación dirigida a mejorar el rendimiento de otras tecnologías LAN, como Token Ring y FDDI. La organiza-

ción interna de los switches de fabricantes distintos a menudo tenía diferencias significativas respecto a la estructura del primer switch EtherSwitch; no obstante, el principio del procesamiento de tramas en paralelo para cada puerto no experimentó ningún cambio.

El empleo extendido de los switches fue estimulado debido a la introducción de tecnologías de conmutación que no requerían el reemplazo del equipo instalado en las redes, incluidos adaptadores, concentradores y el sistema de cableado de la red. Los puertos de conmutación funcionaban en el modo half-dúplex normal; por lo tanto, permitían conexiones transparentes tanto del nodo terminal como del concentrador al organizar el segmento lógico completo.

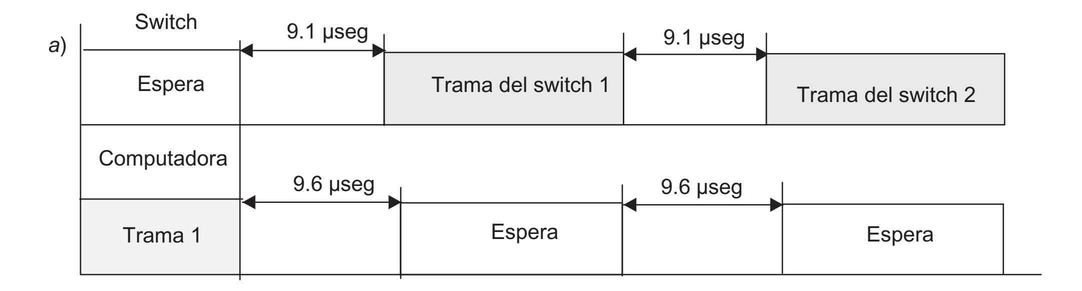
Como los switches y los puentes son transparentes para los protocolos de capa de redes, su introducción en las redes no tuvo influencia en los enrutadores de la red si estaban presentes en aquélla.

15.3.3 Superación de la congestión

En el modo half-dúplex clásico, el switch tendrá la posibilidad de influir en el nodo terminal si emplea los mecanismos del algoritmo de acceso al medio, que debe llevar a cabo el nodo vecino. Se usan dos métodos principales para controlar el flujo de tramas: presión hacia atrás sobre el nodo terminal y captura agresiva del medio.

El método de *presión hacia atrás* consiste en crear colisiones artificiales en el segmento que envía tramas hacia el switch con una intensidad demasiado alta. Para este propósito, el switch suele utilizar una secuencia de congestión, enviada a la salida del puerto al cual el segmento (o nodo) está conectado, para suspender su actividad.

El segundo método para retardar el flujo de tramas se emplea cuando el vecino es un nodo terminal. Este modo se basa en el *comportamiento agresivo del switch del puerto* cuando captura el medio ya sea después de la transmisión de la siguiente trama o luego de la colisión. Estos dos casos se ilustran en la figura 15.13.



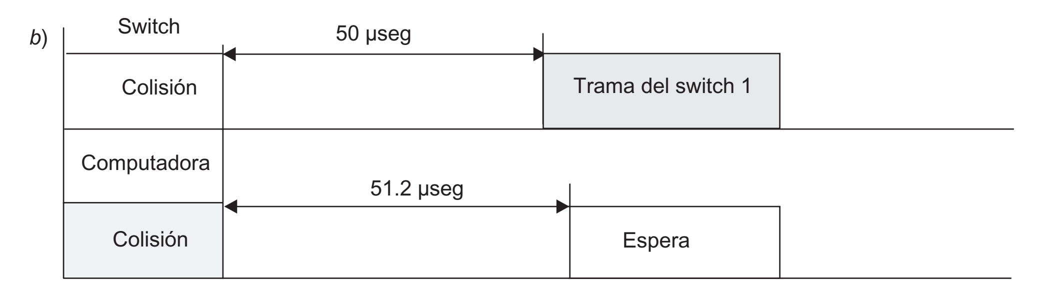


FIGURA 15.13 Comportamiento agresivo del switch en condiciones de sobreflujo del búfer (memoria temporal).

En el primer caso (figura 15.13, *a*), el switch ha terminado la transmisión de la siguiente trama. En lugar de una pausa tecnológica, la cual dura 9.6 µseg, ha hecho una pausa con duración de 9.1 µseg e inició la transmisión de una nueva trama. La computadora no puede capturar el medio, pues mantuvo una pausa estándar con duración de 9.6 µseg y encontró que el medio estaba ocupado.

En el segundo caso (figura 15.13, *b*), las tramas del switch y la computadora chocaron y la colisión se registró. Dado que la computadora después de la colisión hace una pausa de 51.2 µseg, como lo requiere el estándar (el intervalo de retardo tiene intervalos de 512 bits), y el switch hizo pausa durante 50 µseg, la computadora nuevamente no podía transmitir su trama.

El switch podrá utilizar este mecanismo de manera adaptativa si incrementa el nivel de su agresión como sea necesario.

Muchos fabricantes lanzan al mercado mecanismos más complejos de control de congestión al combinar estos dos métodos, los cuales utilizan algoritmos de intercalado de trama basados en las tramas alternadas transmitidas y recibidas. Un algoritmo de intercalado de trama debe ser lo bastante flexible para permitir que el switch transmita en situaciones críticas varias tramas por cada trama recibida, con lo cual descarga su búfer de trama interna, sin disminuir necesariamente la intensidad de la recepción de la trama a cero, sino reduciéndola sólo al nivel requerido.

15.3.4 Traducción de los protocolos de capa de enlace de datos

Los switches pueden traducir un protocolo de la capa de enlace de datos en otro de acuerdo con las especificaciones IEEE 802.1H y RFC 1042, por ejemplo, de Ethernet a FDDI o de Fast Ethernet a Token Ring.

La traducción de los protocolos del LAN se simplifica debido a que no es necesaria la tarea más difícil (la traducción de direcciones) que se lleva a cabo mediante enrutadores y compuertas cuando se conectan redes heterogéneas.

> Todos los nodos terminales de las LAN tienen una dirección única en el mismo formato (direcciones MAC) independiente del protocolo soportado.

Por lo tanto, la dirección del adaptador de red Ethernet es entendida por el adaptador de red FDDI, y ambos nodos pueden utilizar estas direcciones en los campos de sus tramas sin considerar que el nodo con el que interactúan pertenece a una red que funciona con una tecnología diferente.

De lo anterior se deduce que cuando se coordinan protocolos de LAN, los switches no construyen tablas para traducción de direcciones; en su lugar, transfieren las direcciones de las tramas, de fuente y de destino, desde la trama de un protocolo hasta la trama de otro protocolo.

Aparte de cambiar el orden de los bits cuando transmiten bytes de dirección, la traducción de dirección del protocolo Ethernet (y el protocolo Fast Ethernet, que utiliza el mismo formato de trama) para los protocolos FDDI y Token Ring incluye la realización de alguna o todas las operaciones siguientes:

- Calcular las longitudes del campo de datos de la trama y colocar este valor en el campo de longitud (*Length*) cuando se transmite una trama desde una red FDDI o Token Ring hacia una red Ethernet 802.3. (Las tramas FDDI y Token Ring no contienen el campo *Length*.)

- Completar los campos de estado de la trama cuando se transmiten tramas desde una red FDDI o Token Ring hacia una red Ethernet. Las tramas de FDDI y Token Ring tienen dos bits que se establecen mediante la estación para la cual está dirigida la trama: el bit de reconocimiento de dirección (A) y el bit de copia de trama (C). Cuando el switch transmite una trama hacia otra red, no hay reglas estándar para establecer los bits A y C en la trama devuelta por el anillo hacia la estación fuente. Por lo tanto, los fabricantes de switches resuelven este problema a discreción.
- Descartar tramas con un campo de datos mayor que 1 500 bytes y transmitidos desde una red FDDI o Token Ring hacia una red Ethernet, ya que 1 500 bytes es la longitud máxima del campo de datos para Ethernet. Más adelante, al no haber recibido respuesta desde la estación de destino en la red Ethernet, el protocolo de capa superior de la estación fuente en la red FDDI o Token Ring disminuirá posiblemente el tamaño de los datos transmitidos dentro de una sola trama. Después de eso, el switch será capaz de transmitir tramas entre estas estaciones. Otra variante para resolver este problema asegura que el switch soporte fragmentación IP. Sin embargo, esto requiere que el switch implemente un protocolo de capa de red para asegurar que IP sea soportada por los nodos que interactúan en las redes traducidas.
- Completar el campo *Type* (el tipo de protocolo en el campo de datos) de una trama Ethernet II cuando se transmite una trama que llega desde una red que soporta tramas FDDI o Token Ring, donde no existe un campo equivalente. En lugar del campo de tipo (Type), las tramas FDDI y Token Ring tienen campos *DSAP* y *SSAP*, que sirven para el mismo propósito, pero tienen otros códigos para los protocolos designados. Con el fin de simplificar la traducción, la especificación RFC 1042 sugiere utilizar siempre en la red FDDI o Token Ring tramas con encabezados LLC/SNAP, los cuales tienen el mismo campo de tipo (Type) con los mismos valores que las tramas Ethernet II. Cuando se traducen las tramas, los datos desde el campo de tipo del encabezado LLC/SNAP se mueven al campo *Type* de la trama Ethernet II, y viceversa. Si existen distintos formatos de trama de los correspondientes en Ethernet II en la red Ethernet, también deberán tener el encabezado LLC/SNAP.
- Volver a calcular la suma verificadora de la trama de acuerdo con los valores recién formados de los campos de servicio de la trama.

15.3.5 Filtrado del tráfico

Muchos modelos de switch permiten que los administradores especifiquen condiciones adicionales de filtrado de tramas que completen dichas condiciones en su nivel estándar según la información de la tabla de dirección.

> Los **filtros definidos por el usuario** están dirigidos a crear barreras adicionales para las tramas, pero limitan el acceso a servicios de red específicos para ciertos grupos de usuarios.

Los filtros más simples definidos por el usuario son los basados en las direcciones MAC de las estaciones. Como las direcciones MAC son la información con la que trabaja el switch, permite crear tales filtros en una forma conveniente para el administrador de la red. Por ejemplo, pueden especificarse algunas condiciones en un campo adicional de la tabla de dirección, de manera similar a las especificadas en la tabla de dirección del switch mostradas en la figura 15.7 (por ejemplo, tramas descartadas con dirección específica). En este caso, el usuario que trabaja en la computadora con la dirección MAC especificada no tendrá acceso a los recursos de otro segmento de la red.

Muy a menudo, el administrador necesita definir condiciones de filtrado más complejas, por ejemplo, evitar que algún usuario imprima documentos en un servidor de impresión específico de Windows desde otro segmento mientras permite que el usuario tenga acceso a los otros recursos de ese segmento. Para poner en práctica un filtro así, es necesario denegar la transmisión de tramas con una dirección MAC específica, que contenga paquetes SMB encapsulados, si el campo apropiado de ese paquete indica el tipo de servicio de "impresión". Los switches no analizan los protocolos de capa superior, como SMB; por consiguiente, el administrador, para especificar condiciones de filtrado, debe determinar de modo manual el campo cuyo valor se debe filtrar. Dicho filtro está especificado en la forma del par de "tamaño de compensación" ("offset size") respecto a la posición de inicio del campo de datos de la trama de capa de enlace de datos, después de lo cual es necesario especificar el valor hexadecimal de este campo correspondiente al servicio de impresión.

Por lo regular, las condiciones de filtrado están escritas como expresiones booleanas, formadas mediante el uso de los operadores `AND` y `OR`.

15.3.6 Arquitectura y diseño del switch

En la actualidad, para acelerar las operaciones de conmutación, todos los switches utilizan LIC especializados: ASIC optimizado para llevar a cabo operaciones de conmutación. Con frecuencia, un solo switch tiene varios LIC especializados, cada uno de los cuales realiza un conjunto de operaciones funcionalmente completo.

Aparte de los chips o circuitos integrados de procesador especializados, la operación con éxito en modo sin bloqueo requiere que el switch esté equipado con una unidad rápida para transmitir tramas entre los circuitos integrados o chips de procesador de sus puertos.

En la actualidad, los switches utilizan uno de los tres métodos básicos para construir una unidad de intercambio de esta clase:

- Matriz de conmutación
- Bus común
- Memoria compartida de puertos múltiples

Muy a menudo, estos tres métodos están combinados dentro del mismo switch.

La **matriz de conmutación** asegura la manera más simple de interacción entre procesadores del puerto. Este método fue implementado en el primer segmento de producción de un switch de LAN. Empero, la implementación de la matriz de esa conmutación sólo es posible para un número de puertos predefinido y limitado, y la complejidad del diseño crece de manera proporcional al cuadrado de la cantidad de puertos del switch (figura 15.14).

Una representación más detallada de una variante de la implementación de la matriz de conmutación dirigida a soportar ocho puertos se encuentra en la figura 15.15. Las unidades de entrada de los procesadores de puerto, basados en el examen de las tablas de dirección del switch, determinan el número del puerto de salida mediante la dirección del destino; agregan esta información a los bytes de la trama fuente en la forma de una etiqueta especial. En este ejemplo, por simplicidad, la etiqueta es un número binario de 3 bits correspondiente al número del puerto de salida.

La matriz consta de tres niveles de switches binarios que conectan su entrada a una de las dos salidas según el valor del bit de la etiqueta. Los switches del primer nivel están controlados por el primer bit de la etiqueta, los switches del segundo nivel se controlan mediante el segundo bit y los switches de la tercera capa están bajo el control del tercer bit.

La matriz puede ponerse en práctica de otras maneras con base en otros tipos de diseños combinatorios. No obstante, la tecnología de los enlaces físicos de conmutación mantiene

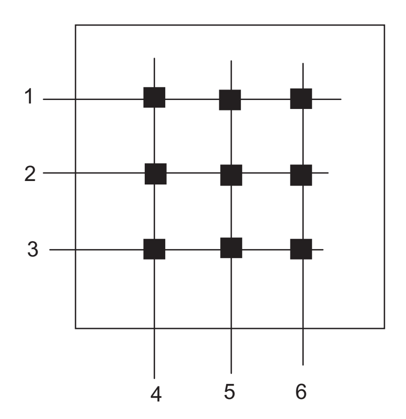


FIGURA 15.14 Matriz de conmutación.

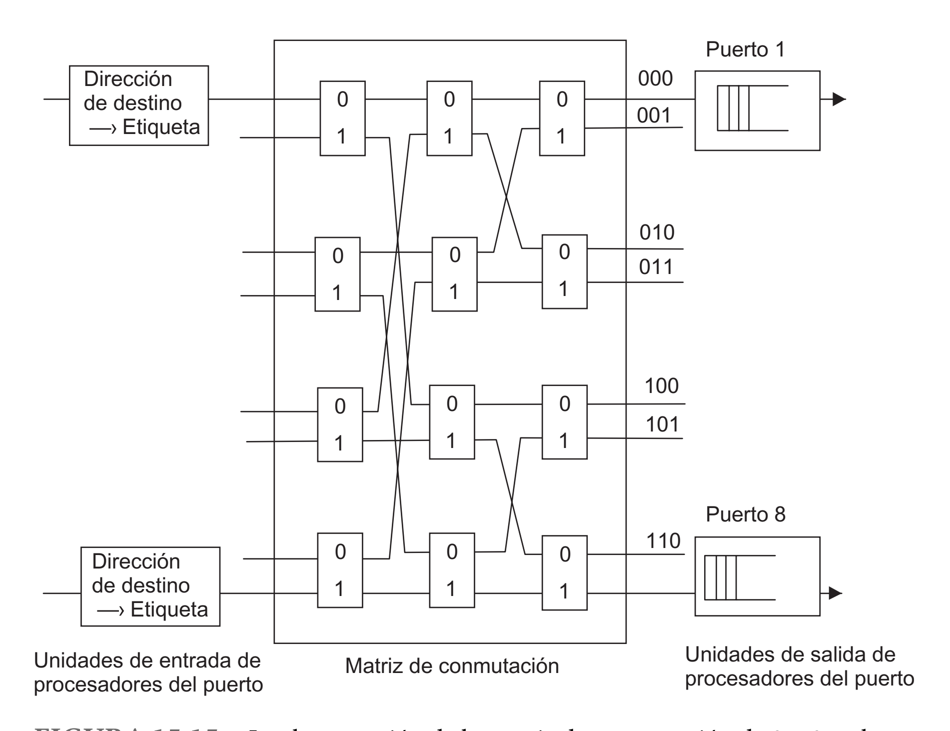


FIGURA 15.15 Implementación de la matriz de conmutación de 8 × 8 en la que se usan switches binarios.

su característica específica. La desventaja ya conocida de esta tecnología es la ausencia de almacenamiento temporal de los datos dentro de la matriz de conmutación. De este modo, si el circuito no puede formarse debido a que el puerto de salida del elemento o elementos de conmutación intermedio(s) se encuentra(n) ocupado(s), los datos deben acumularse dentro de la fuente de los datos, cuyo papel en este caso lo realiza la unidad de entrada del puerto que recibió la trama. Las ventajas principales de dichas matrices incluyen la alta velocidad de conmutación y la estructura regular, la cual es conveniente para implementar en las LIC. No obstante, después de implementar la matriz de $N \times N$ como parte de un LIC, es evidente otra desventaja: la dificultad en incrementar el número de puertos conmutados.

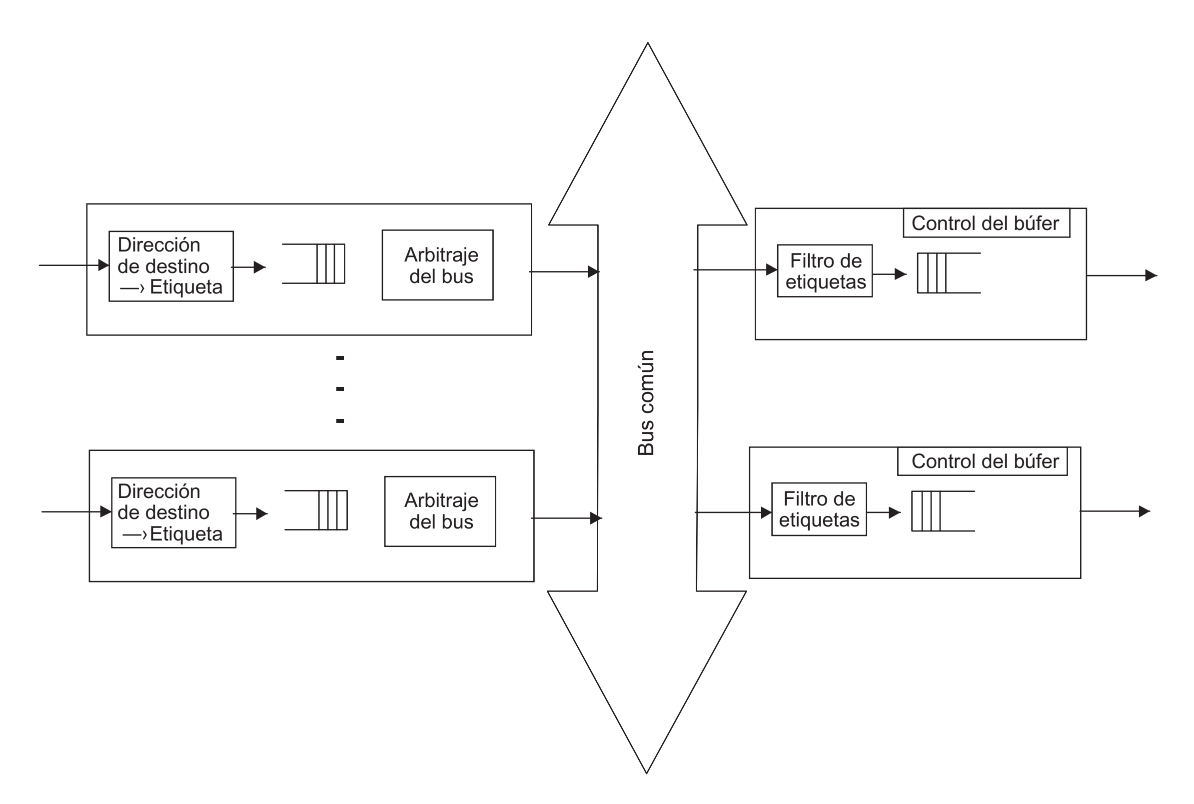


FIGURA 15.16 Arquitectura de un switch basada en un bus común.

En los switches basados en un **bus común**, los procesadores del puerto están conectados mediante un bus común de alta velocidad utilizado en el modo de partición de tiempo.

Un ejemplo de tal arquitectura se observa en la figura 15.16. Para asegurar que el bus no bloquee la operación de conmutación, es necesario garantizar que su rendimiento sea por lo menos la suma del rendimiento de todos los puertos del switch. Para switches modulares, algunas combinaciones de módulos con puertos de baja velocidad pueden producir una operación sin bloqueo, y la instalación de módulos con puertos de alta velocidad puede generar el modo en el cual el bus común se convierta en un cuello de botella.

La trama debe transmitirse a través del bus en partes pequeñas, constituidas por varios bytes, para hacer la transmisión de los datos entre los puertos parte de un modo seudoparalelo sin incluir retardos en la transmisión de la trama como un todo. El tamaño de una celda de datos de tal clase lo determina el fabricante del switch. Algunos fabricantes eligen una celda ATM con la longitud de su campo de datos de 48 bytes como la parte de los datos transmitida a través del bus por operación. Un enfoque de este tipo simplifica la traducción de los protocolos de LAN en el protocolo ATM si el switch soporta estas tecnologías.

La unidad de entrada del procesador complementa la celda transportada mediante el bus con una etiqueta en la cual especifica el número del puerto de destino. Cada unidad de salida del procesador de puerto contiene el filtro de etiquetas que selecciona las etiquetas dirigidas a este puerto.

Al igual que la matriz de conmutación, el bus no puede llevar a cabo almacenamiento temporal intermedio; a pesar de ello, como los datos de la trama se dividen en pequeñas celdas, este método es libre de retardos relacionados con la espera inicial para la disponibilidad del puerto de salida: el método de conmutación del paquete se incrementa aquí en lugar del método de conmutación de circuito.

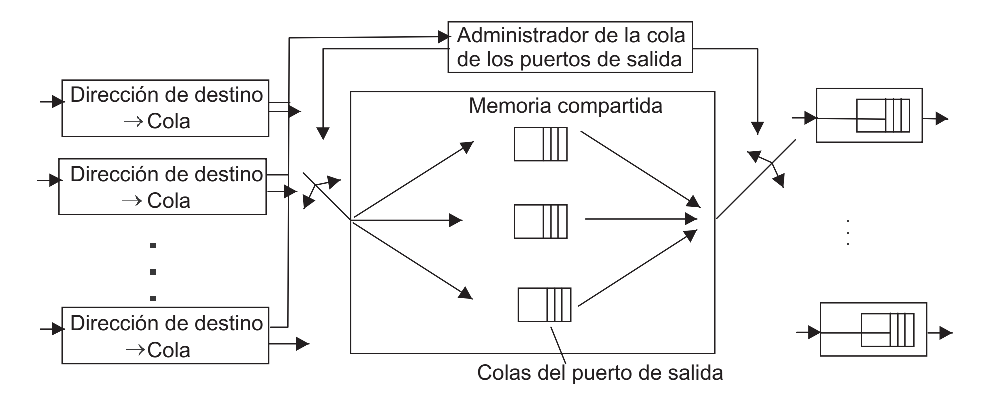


FIGURA 15.17 Arquitectura de un switch basada en memoria compartida.

La tercera arquitectura básica para interacción del puerto es una **memoria compartida**. Un ejemplo de tal arquitectura se proporciona en la figura 15.17.

Las unidades de entrada de los puertos del procesador están conectadas a la entrada conmutada de la memoria compartida, y las unidades de salida de los procesadores están conectadas a la salida conmutada de esta memoria. El administrador de la cola de los puertos de salida controla la conmutación de la entrada y salida de la memoria compartida. Dentro de la memoria compartida, este administrador organiza varias colas de datos, una cola por puerto de salida. Las unidades de entrada de los procesadores pasan al administrador solicitudes para escribir los datos en la cola del puerto correspondiente a la dirección de destino de la trama. El administrador de la cola en turno conecta la entrada de la memoria a una de las unidades de entrada del procesador, y esa unidad escribe parte de los datos de la trama en la cola del puerto de salida específico. A medida que se llenan las colas, el administrador en turno conecta la salida de la memoria compartida a las unidades de salida de los puertos del procesador, y los datos de las colas se escriben en los búferes de salida de los procesadores.

Se usa la memoria temporal o de búfer común, distribuida de manera flexible por el administrador entre los puertos individuales, con el fin de reducir los requerimientos para el tamaño de memoria temporal o del búfer del procesador del puerto. No obstante, la memoria debe ser lo suficientemente rápida para soportar la velocidad de la transmisión de datos entre los *N* puertos del switch.

Switches combinados

Cada una de las arquitecturas descritas tiene ventajas y desventajas; por lo tanto, en switches complejos, estas arquitecturas se utilizan a menudo en combinación. Un ejemplo de una arquitectura combinada de este tipo se ilustra en la figura 15.18.

El switch consta de módulos con números fijos de puertos (2-12), implementados con base en un LIC especializado que pone en marcha la arquitectura de una matriz de conmutación. Si los puertos entre los cuales es necesario transmitir una trama de datos pertenecen al mismo módulo, la transmisión de la trama se lleva a cabo mediante los procesadores del módulo según indica la matriz de conmutación del módulo. Si los puertos pertenecen a módulos diferentes, los procesadores se comunican por medio del bus común. Con una arquitectura así, la transmisión de los datos dentro de un módulo tendrá lugar más rápidamente que la transmisión entre módulos, pues la matriz de conmutación proporciona el método más rápido de interacción entre puertos, aunque este método es el menos escalable. La velocidad

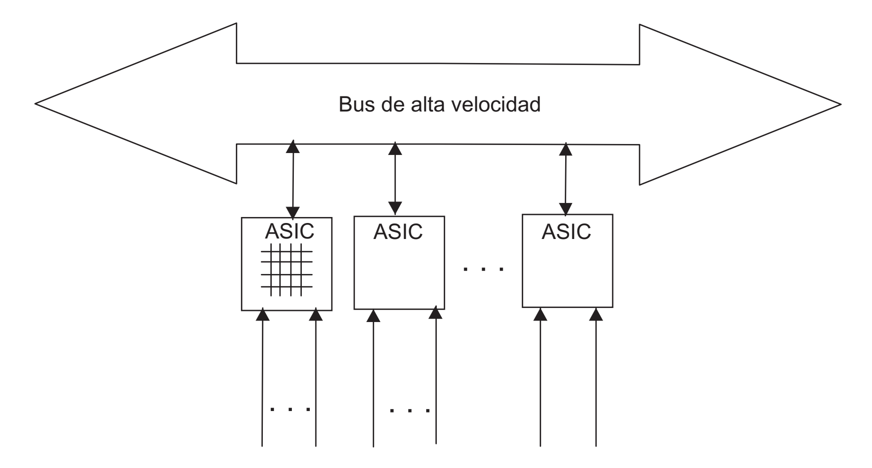


FIGURA 15.18 Arquitectura de un switch combinado basada en una matriz de conmutación y un bus común.

del bus interno de un switch puede alcanzar varios gigabits por segundo, y algunos modelos potentes tienen la velocidad de bus de decenas de gigabits por segundo.

También son posibles otros métodos de arquitecturas combinadas; por ejemplo, la memoria compartida puede utilizarse para organizar la interacción entre los módulos.

15.3.7 Características del desempeño de switches

La velocidad de filtrado y la velocidad de direccionamiento son las dos características de rendimiento más importantes de un switch. Éstas constituyen parámetros integrales pues no dependen de la implementación técnica de un switch.

La *velocidad de filtrado* define la velocidad a la que el switch lleva a cabo las etapas de procesamiento de la trama:

1. Cargar la trama en el búfer interno.
2. Examinar la tabla de dirección para hallar el puerto para la dirección de destino de la trama.
3. Descartar las tramas para las cuales los puertos fuente y de destino pertenecen al mismo segmento lógico.

La velocidad de filtrado para prácticamente todos los switches es sin bloqueo, pues el switch tiene tiempo para descartar tramas a la misma velocidad a la que llegan.

La *velocidad de direccionamiento* es la velocidad a la cual el switch lleva a cabo las siguientes etapas del procesamiento de la trama:

1. Cargar la trama en el búfer interno.
2. Considerar la tabla de dirección con el fin de encontrar el puerto para la dirección de destino de la trama.
3. Pasar la trama a la red mediante el uso del puerto encontrado en la tabla de dirección.

La velocidad de filtrado y la velocidad de direccionamiento se miden por lo general en tramas por segundo. Si las características del switch se facilitan sin especificar el protocolo y tamaño de trama para los cuales se proporcionan los valores de las velocidades de filtrado

y direccionamiento, de manera predeterminada, estos parámetros los especifican el protocolo internet y las tramas de tamaño mínimo; por ejemplo, 64 bytes. Las tramas de la longitud mínima siempre crean el modo de operación más difícil para el switch en comparación con las tramas de otro formato a la misma velocidad de datos del usuario. Debido a esto, cuando se prueba el switch, se utilizan el modo de transmisión de trama de datos de longitud mínima como la prueba más compleja dirigida a verificar de manera adicional la capacidad del switch para funcionar bajo la peor combinación de parámetros de tráfico.

El *retardo de transmisión de la trama* se mide como el tiempo transcurrido desde la llegada del primer byte de la trama al puerto de entrada del switch hasta que este byte aparece en el puerto de salida del switch. El retardo de transmisión de la trama consta del tiempo requerido para el almacenamiento temporal de la trama y el tiempo gastado para el procesamiento de la trama por el switch, incluida la exterminación de la tabla de dirección, la decisión de filtrado para dirigir la trama y el acceso al medio del puerto de salida.

El rendimiento del switch es el número de datos del usuario transmitidos por unidad de tiempo a través de sus puertos (medido en megabits por segundo). Como el switch funciona en la capa de enlace de datos, desde su punto de vista, los datos del usuario son los transportados en el campo de datos de las tramas que pertenecen a los protocolos de la capa de enlace de datos: Ethernet, Token Ring, FDDI, etc. El valor máximo del rendimiento del switch se obtiene siempre en las tramas de longitud máxima, pues al compartir el encabezado de la información del servicio de trama es significativamente menor que para las tramas de longitud mínima. El switch es un dispositivo de puertos múltiples; por lo tanto, una práctica común consiste en proporcionar su característica de rendimiento principal como el rendimiento total del switch durante la transmisión de tráfico simultáneo a través de todos sus puertos.

El método de transmisión de trama (al vuelo o con almacenamiento temporal o búfer completo) influye en el desempeño del switch. Los switches que transmiten tramas al vuelo introducen los retardos de transmisión de trama más pequeños por cada switch de tránsito. Por consiguiente, la reducción total del retardo en la entrega de los datos puede ser bastante significativo, lo cual es importante para el tráfico multimedia. Además, el método de conmutación seleccionado influye en las posibilidades de implementar varias funciones auxiliares útiles, por ejemplo, traducir los protocolos de capa de enlace de datos.

La tabla 15.1 muestra una comparación de los dos métodos de conmutación.

El retardo promedio de los switches que funcionan al vuelo bajo una carga considerable ocurre porque el puerto de salida a menudo está ocupado recibiendo otra trama; por lo tanto, la trama recién llegada al puerto actual tiene que almacenarse temporalmente.

El switch que funciona al vuelo puede verificar la exactitud de las tramas que se transmiten, pero es incapaz de descartar la trama corrompida de la red, porque parte de sus bytes (como regla, la mayoría de ellos) ya se han transmitido en la red.

NOTA *Debido a que cada método tiene sus ventajas y desventajas, los modelos de switch que no deben traducir protocolos a veces ponen en marcha el mecanismo de cambiar de manera adaptativa el modo de operación del switch. El modo principal de un switch de esta naturaleza es la conmutación al vuelo, pero el switch controla constantemente el tráfico. Cuando las tramas corrompidas llegan a ser más frecuentes y su intensidad excede cierto umbral, el switch cambia el modo al de almacenamiento temporal completo. Más tarde, el switch puede regresar al anterior modo "al vuelo".*

Otra característica importante designada de cualquier switch es el **tamaño máximo de la tabla de dirección**. Define el número máximo de direcciones MAC con las que el switch puede trabajar de manera simultánea.

TABLA 15.1 Capacidades funcionales de conmutación al vuelo y con almacenamiento temporal total

Función	Al vuelo	Con almacenamiento temporal total
Protección contra corrupción de tramas	No	Sí
Soporte para redes heterogéneas (Ethernet, Token Ring, FDDI y ATM)	No	Sí
Retardo de transmisión de tramas	Bajo (5-40 µseg) para carga baja; medio para carga intensa	Medio para cualquier carga
Soporte para enlaces reservados	No	Sí
Función de análisis de tráfico	No	Sí

Con mayor frecuencia los switches utilizan la unidad de procesamiento dedicada para llevar a cabo las operaciones de cada puerto, y cada unidad de procesamiento está equipada con la memoria para almacenar su copia de la tabla de dirección. Cada puerto almacena sólo aquellos datos con los que ha trabajado más recientemente, por lo cual las copias de las tablas de dirección de diferentes unidades de procesamiento suelen contener distinta información de dirección.

El valor del número máximo de direcciones MAC que pueden almacenarse en la memoria del puerto del procesador depende del área de aplicación del switch. Los switches de grupos de trabajo por lo general soportan varias direcciones por puerto, porque están dirigidos a crear microsegmentos. Los switches de nivel departamental deben soportar cientos de direcciones y los switches troncales han de soportar miles de direcciones, por lo regular entre 4 000 y 8 000.

El tamaño insuficiente de una tabla de dirección puede hacer más lenta la operación del switch e inundar la red con tráfico innecesario. Si se llena la tabla de dirección del procesador del puerto y éste encuentra una nueva dirección en la trama que acaba de llegar, el procesador deberá descartar de la tabla algunas direcciones antiguas y reemplazarlas con la nueva. Esta operación gasta algo del tiempo del procesador, pero las principales pérdidas del rendimiento tendrán lugar después de la llegada de la trama que contiene la dirección de destino que debió eliminarse de la tabla de dirección. Como la dirección de destino de la trama se ha olvidado, el switch debe transmitirla a todos los otros puertos.

A fin de resolver dicho problema, algunos fabricantes de switches cambian el algoritmo utilizado para procesar las tramas con direcciones de destino olvidadas. Uno de los puertos está configurado como un puerto troncal hacia el que todas las tramas con direcciones desconocidas se pasan de manera predeterminada.[1]

[1] En los enrutadores, una técnica así se ha utilizado desde hace tiempo, al permitir que los tamaños de las tablas de dirección se reduzcan en una red organizada de acuerdo con el principio de jerarquías.

Se transmitirá una trama hacia el puerto troncal si este puerto está conectado al que mantiene una posición superior en la jerarquía de una red a gran escala y tiene suficiente volumen de tabla de dirección, lo cual permite saber dónde debe transmitirse cada trama.

15.4 PROTOCOLOS DE LAN FULL-DÚPLEX

PALABRAS CLAVE: microsegmentación, dominio de colisión, 106Base-X, 106Base-R, 106Base-W y 106Base-LX4.

15.4.1 Cambios introducidos en la capa MAC por la operación en modo full-dúplex

La tecnología de conmutación no está relacionada de manera directa con el método de acceso al medio utilizado por los puertos del switch. Cuando un segmento que representa un medio compartido se conecta a un puerto de switch, este puerto debe soportar el modo half-dúplex, como cualquier otro modo de este segmento.

No obstante, cuando en vez del segmento entero sólo una computadora está conectada a cada puerto del switch y esta conexión utiliza dos canales físicamente separados, lo cual es aplicable para casi todos los estándares Ethernet con excepción de las versiones de Ethernet coaxial, la situación deja de ser tan inequívoca. El puerto puede funcionar en el modo half-dúplex normal además del modo full-dúplex.

La conexión de computadoras individuales a puertos del switch en lugar de segmentos se conoce como *microsegmentación*.

En el modo de operación half-dúplex, que es normal para Ethernet, el puerto del switch continúa la detección de colisiones. En este caso, el dominio de colisión es una sección de la red que incluye el transmisor del switch, el receptor del switch, el transmisor del adaptador de red de la computadora y los cables de par trenzado que conectan los transmisores a los receptores (figura 15.19).

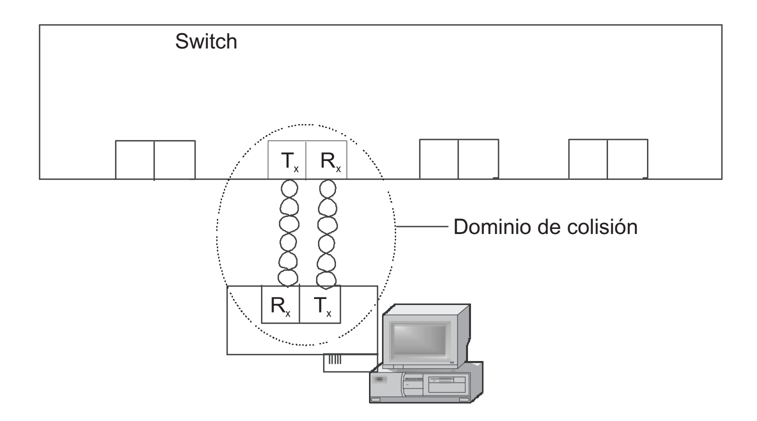


FIGURA 15.19 Dominio de colisión creado por una computadora y un puerto de switch.

La colisión tiene lugar cuando los transmisores del puerto del switch y el adaptador de la red comienzan la transmisión de sus tramas de manera casi simultánea, asumiendo que el segmento está libre (véase la figura 15.19). Aunque la probabilidad de colisión en un segmento así es mucho más pequeña que en un segmento que consta de 20 a 30 nodos, esta probabilidad no es igual a cero. Al mismo tiempo, el rendimiento máximo del segmento Ethernet es de 14 880 tramas por segundo para la longitud de trama mínima y se comparte entre el transmisor del puerto del switch y el transmisor del adaptador de red. Suponiendo que se divide en partes iguales, cada transmisor tiene la posibilidad de transmitir cerca de 7 440 tramas por segundo.

En el modo full-dúplex, la transmisión simultánea de los datos por el switch del puerto y el adaptador de red no se considera colisión. Principalmente, este modo de operación es natural para canales de comunicaciones full-dúplex individuales y se utiliza con frecuencia en protocolos WAN. En el caso de conexión full-dúplex, los puertos Ethernet de 10 Mbps pueden transmitir datos a la velocidad de 20 a 10 Mbps en cada dirección.

Como resulta evidente, es necesario asegurar que las capas MAC de los dispositivos que interactúan soportan este modo especial. Cuando sólo el primer nodo soporta el modo full-dúplex, otro nodo registraría colisiones de manera constante y suspendería su operación, y el segundo nodo continuaría transmitiendo los datos, que nadie recibe en ese momento. Las modificaciones que se deben hacer en la lógica de operación de la capa MAC del nodo con el fin de habilitarlo para que funcione en el modo full-dúplex son mínimas. Sólo se debe cancelar el registro y procesamiento de colisiones en las redes Ethernet. En las redes Token Ring y FDDI, el adaptador de red y el puerto del switch deben enviar sus tramas sin esperar la llegada de la señal o token de acceso, en cualquier momento que el nodo terminal lo necesite. En realidad, cuando funciona en modo full-dúplex, la capa MAC del nodo ignora el método de acceso al medio diseñado para una tecnología específica.

> Cuando se idearon las nuevas tecnologías Fast Ethernet y Gigabit Ethernet, el modo full-dúplex obtenía derechos absolutos y se convirtió en uno de los modos estándar de operación de nodo de red. Actualmente, los adaptadores de red pueden soportar ambos modos de operación, para lo cual utilizan el algoritmo de acceso CSMA/CD cuando se conectan al puerto del concentrador y funcionan en el modo full-dúplex cuando se conectan al puerto del switch.

15.4.2 Problemas de control de congestión en el modo full-dúplex

El simple abandono del soporte del algoritmo de acceso al medio compartido sin modificación del protocolo aumenta la probabilidad de pérdida de tramas en los switches, pues se pierde el control sobre los flujos de tramas enviados por los nodos terminales hacia la red. En el modo half-dúplex, típico para las redes de medios compartidos, el flujo de tramas estaba regulado por el método de acceso al medio compartido. Después de la migración al modo full-dúplex, se permite al nodo enviar tramas al switch cuando lo necesite; por lo tanto, cuando se funciona en este modo, los switches de la red pueden congestionarse y no tener medios de retrasar el flujo de tramas.

Por lo regular, la congestión no es causada por el switch bloqueado (es decir, por el rendimiento insuficiente de sus procesadores para dar servicio al flujo de tramas). La verdadera razón de la congestión reside en el limitado ancho de banda de un puerto de salida específico, el cual está definido por los parámetros del protocolo.

Por lo tanto, si el tráfico entrante se encuentra distribuido de manera desigual entre los puertos de salida, será fácil imaginar una situación en la que el tráfico con máxima intensidad

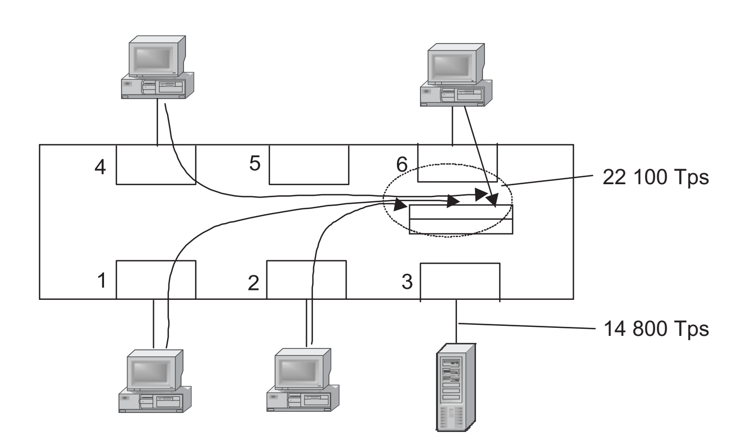


FIGURA 15.20 Sobreflujo del búfer del puerto debido a tráfico desequilibrado.

que exceda el máximo del protocolo se dirija a alguno de los puertos de salida del switch. Una situación de esta naturaleza se ilustra en la figura 15.20. Aquí, el flujo de tramas de 64 bytes desde los puertos 1, 2, 4 y 6, con una intensidad total de 20 100 tramas por segundo, está dirigido al puerto 3 del switch Ethernet. Dicho puerto tiene una carga de 150%. Naturalmente, cuando las tramas llegan al búfer del puerto a la velocidad de 20 100 tramas por segundo y abandonan el puerto a la velocidad de 14 880 tramas por segundo, el búfer interno del puerto de salida se llenará poco a poco con tramas sin procesar.

No es difícil calcular que, en este ejemplo, una memoria temporal o búfer de 100 KB se llenará en 0.22 segundos después de que inicie su operación (un búfer de este tamaño puede almacenar hasta 1 600 de 64 bytes). El incremento del tamaño del búfer a 1 MB aumentará el tiempo de llenado del mismo a 2.2 segundos, lo que tampoco es aceptable.

Dicho problema podrá resolverse si se emplean métodos de control de congestión considerados en el *capítulo 7*.

Como se recordará, existen diferentes tipos de herramientas de control de congestión: administración de colas en switches, retroalimentación y reservación de ancho de banda. Con base en estas herramientas, es posible crear un sistema eficaz de soporte QoS para diferentes clases de tráfico.

En esta sección se considerará el mecanismo de retroalimentación estandarizado para Ethernet en marzo de 1997 como la especificación IEEE 802.3x. El mecanismo de retroalimentación IEEE 802.3x se utiliza únicamente en el modo dúplex de la operación del puerto del switch. Este mecanismo es muy importante para switches LAN, pues permite que las pérdidas de tramas se reduzcan debido al sobreflujo del búfer, si la red asegura un soporte QoS diferenciado para distintas clases de tráfico o proporciona solamente servicio del mejor esfuerzo. Otros mecanismos de QoS se examinarán en el siguiente capítulo.

La especificación 802.3x introduce una nueva subcapa en la pila de protocolo Ethernet: la subcapa de control MAC, la cual se localiza por arriba de la capa MAC y es opcional (figura 15.21).

Las tramas de esta subcapa pueden emplearse para varios propósitos. No obstante, por el momento, sólo una tarea está definida para ellas en los estándares de Ethernet: suspender la transmisión de la trama por los otros nodos durante un tiempo específico.

La trama de control MAC es diferente de las tramas de datos del usuario en que su campo *Type/Length* siempre contiene el valor hexadecimal 88-08. Dicha trama está destinada para su aplicación universal; por lo tanto, tiene un formato bastante complejo (figura 15.22).

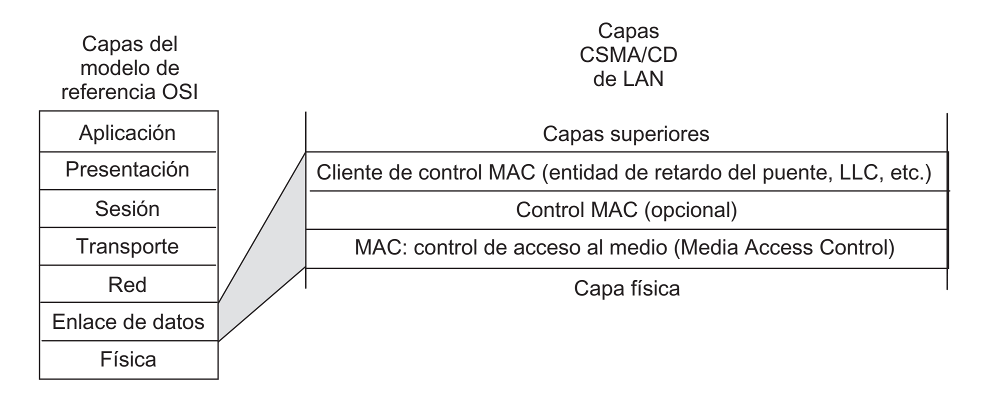


FIGURA 15.21 Subcapa de control MAC.

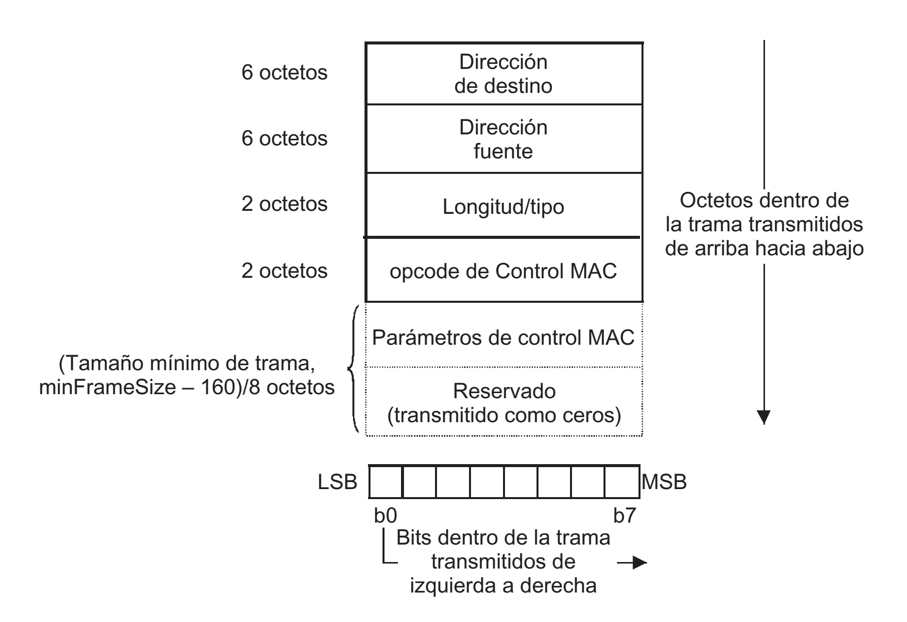


FIGURA 15.22 Formato de trama del control MAC .

El switch utiliza la trama de control MAC cuando se necesita para suspender temporalmente la llegada de tramas desde el nodo vecino para descargar sus colas internas.

Como una dirección de destino, es posible emplear la dirección de emisión múltiple reservada para este propósito: 01-80-C2-00-00-01. Este enfoque es conveniente cuando el nodo vecino también es un switch (pues los puertos del switch no tienen direcciones MAC únicas). Si el vecino es un nodo terminal, también se puede utilizar la dirección MAC única.

El campo OPCODE de Control MAC especifica el código de la operación de control. Como ya se mencionó, solamente se ha definido una operación: se conoce como PAUSE ("PAUSA") y tiene el código hexadecimal 00-01.

El campo MAC Control Parameters (Parámetros de Control de MAC) especifica el tiempo para el cual el nodo que recibe un código de esta clase debe suspender la transmisión de tramas hacia el nodo que ha enviado la trama con la operación PAUSE. La unidad de

tiempo es de intervalos de 512 bits para la implementación Ethernet particular; la cantidad de suspensión posible abarca desde 0 hasta 65 535.

Como se deduce de dicha expresión, este mecanismo de retroalimentación está relacionado con el tipo 2 de Retroalimentación, de acuerdo con la clasificación proporcionada en el capítulo 7. También tiene sus características específicas, pues en mecanismos de este tipo se emplean por lo regular dos operaciones: suspender la transmisión de la trama y reanudarla. Tal es el mecanismo implementado en uno de los más antiguos protocolos de redes de paquetes conmutados: en el protocolo X.25, conocido como LAP-B.

15.4.3 Ethernet 10G

El estándar Ethernet 10G define únicamente el modo full-dúplex de operación; por lo tanto, puede emplearse solamente en LAN conmutadas.

Formalmente, este estándar se designa como IEEE 802.3ae y es un complemento para el texto principal del estándar 802.3. Dicho complemento a la familia Ethernet describe siete nuevas especificaciones de capa física que interactúan con la capa MAC al usar una nueva variante de la subcapa de reconciliación (figura 15.23). Esta subcapa proporciona todas las variantes de la capa física de Ethernet 10G con una interfase unificada que se conoce como Interfaz Independiente para el Medio Gigabit Extendida (XGMII, Extended Gigabit Medium Independent Interface), que atiende las necesidades del intercambio paralelo mediante 4 bytes que forma para flujos de datos.

Como se aprecia en la figura 15.23, existen tres grupos de interfaces físicas del estándar Ethernet 10G: 10GBase-X, 10GBase-R y 10GBase-W. Difieren en el método de codificación utilizado: el método 10GBase-X usa el código 8B/10B, mientras que los otros dos grupos emplean el código 64B/66B. Todas las variantes emplean un medio óptico para la transmisión de datos.

El grupo 10GBase-X consta de una sola interfaz de la subcapa del medio físico dependiente (PMD, Physical Medium Dependent): 10GBase-LX4. El carácter L especifica que la información se transmite por medio de longitudes de onda del segundo intervalo de transparencia (es decir, 1 310 nm). La información se transmite de manera simultánea en cada dirección, para lo cual se usan cuatro ondas (lo que se refleja por medio del dígito 4 en el nombre de la interfaz), que son multiplexadas con apego a la técnica de multiplexado por división de longitud de onda (WDM) (figura 15.24). Cada uno de los cuatro flujos de XGMII se transmite en la fibra óptica a una velocidad de 2.5 Gbps.

La distancia máxima entre el transmisor y el receptor de acuerdo con el estándar 10GBase-LX4 basado en fibra multimodal es de 200 a 300 m (según el ancho de banda de la fibra); para fibra en modo simple, la distancia máxima es de 10 km.

Cada uno de los grupos 10GBase-W y 10GBase-R consta de tres variantes de la subcapa PMD (S, L y E), lo cual depende de la longitud de onda empleada para transmitir la información (850 nm, 1 310 nm y 1 550 nm, respectivamente). Así, existen las siguientes interfaces: 10GBase-WS, 10GBase-WL, 10GBase-WE, 10GBase-RS, 10GBase-RL y 10GBase-RE. Cada una de ellas transmite información por medio de una onda sencilla del intervalo apropiado.

La diferencia entre el grupo 10GBase-W y el grupo 10GBase-R reside en que las interfaces físicas del grupo W aseguran una velocidad de transmisión de datos y un formato de datos compatible con la interfaz Sonet STS-192/SDH STM-64. El ancho de banda de las interfaces del grupo W es de 9.95328 Gbps y la velocidad efectiva de transmisión de datos es de 9.58464

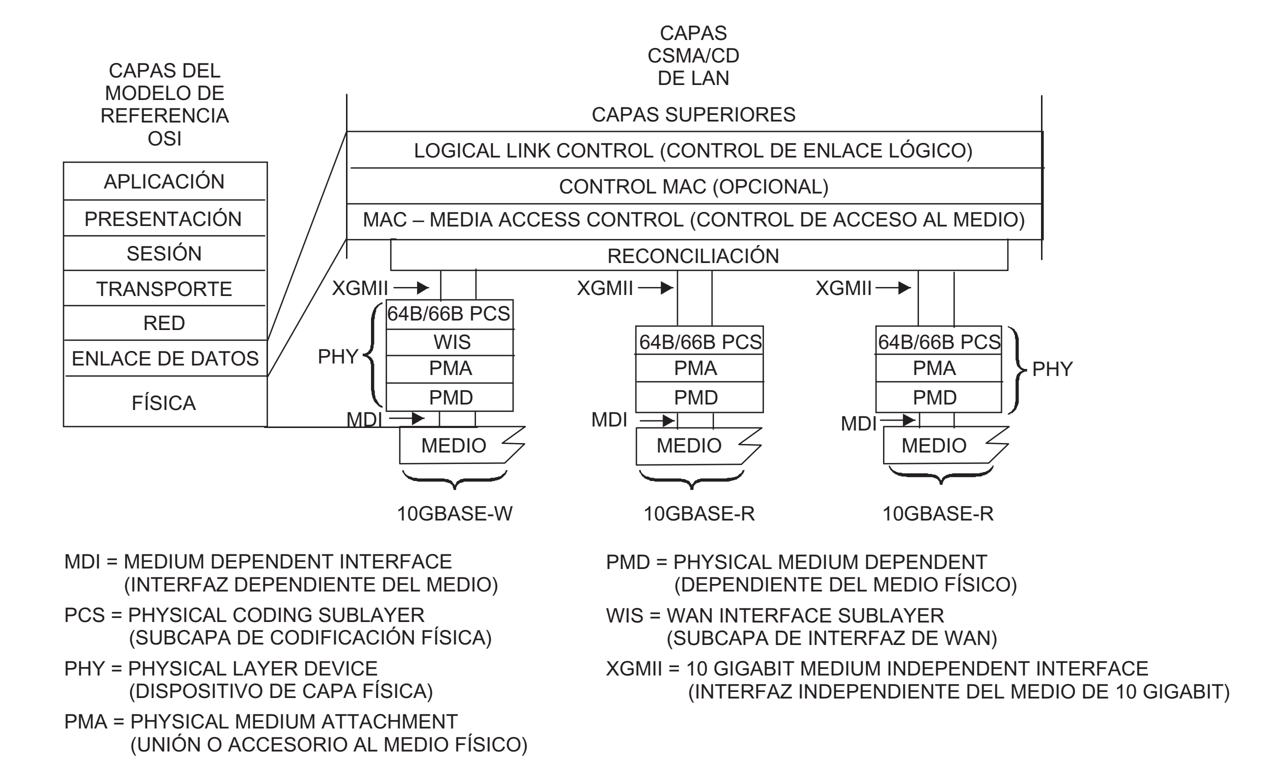


FIGURA 15.23 Tres grupos de interfaces físicas 10G.

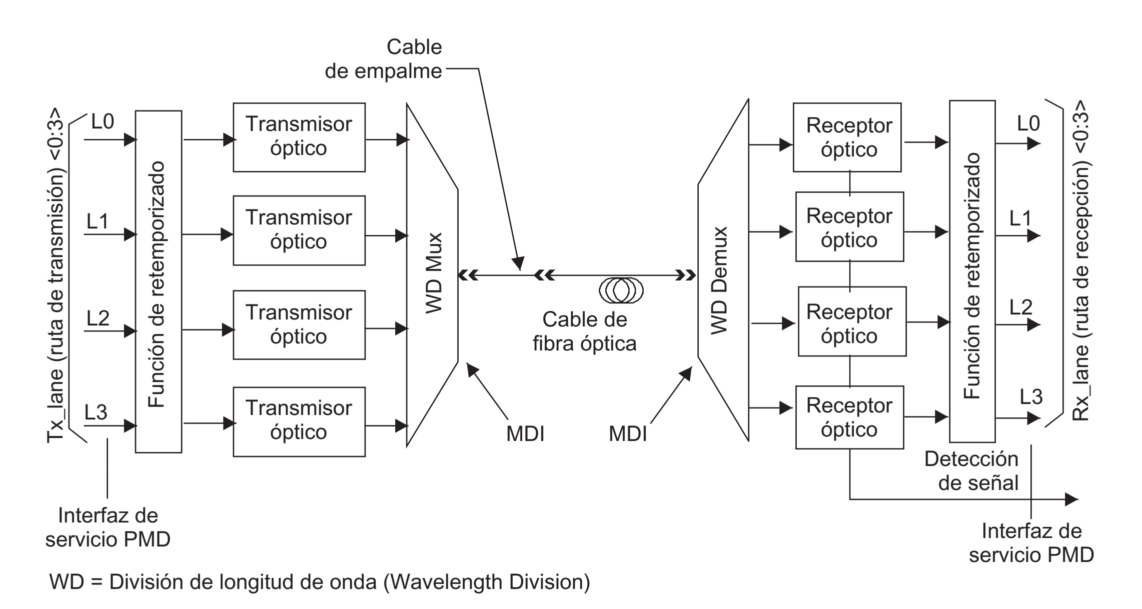


FIGURA 15.24 Interfaz 10GBase-LX4 que utiliza la técnica WDM.

Gbps (parte del ancho de banda lo usan los encabezados de trama STS/STM). Debido a que la velocidad de información para este grupo de interfaces es inferior a 10 Gbps, éstas pueden interactuar únicamente con otra más, lo que significa que la conexión de interfaces como 10GBase-RL y 10GBase-WL es imposible.

Por características eléctricas, las interfaces del grupo W no son totalmente compatibles con las SONET/SDH de velocidades respectivas. Por lo tanto, para establecer la conexión entre redes Ethernet 10G mediante el empleo de la red de transmisión SONET/SDH, los multiplexores de la red de transmisión deben equiparse con interfaces especiales 10G compatibles con las especificaciones 10GBase-W. El soporte de la velocidad de 9.95328 Gbps por el equipo 10GBase-W asegura la posibilidad de transmisión del tráfico Ethernet 10G al utilizar la red SONET/SDH en tramas STS-192/STM-64.

Las interfaces físicas que funcionan en la ventana de transparencia E aseguran la transmisión de los datos a distancias de hasta 40 km. Esto permite crear no sólo las LAN sino también MAN, lo que se refleja en las correcciones al texto fuente del estándar 802.3.

RESUMEN

- La estructura lógica de la red es necesaria cuando se construyen redes de tamaño mediano y grande. Es aceptable usar un medio compartido común solamente para una red que conste de cinco a 10 computadoras.
- La división de una red en segmentos lógicos mejora su desempeño, confiabilidad, flexibilidad y manejo.
- Para la estructuración lógica de los puentes de red y sus sucesores, se utilizan los switches. Esto divide la red en segmentos lógicos empleando pocas herramientas, únicamente sobre la base de los protocolos de capa de enlace de datos. Aparte de ello, estos dispositivos no requieren configuración.
- El método pasivo utilizado por los switches para construir tablas de dirección rastrea el tráfico que pasa. Esto hace imposible operar en una red que contenga ciclos o loops cerrados. Otra desventaja de las redes basadas en switches es la carencia de protección en contra de tormentas de difusión, que estos equipos han de transmitir debido a sus algoritmos de operación.
- El uso de switches permite a los adaptadores de la red usar el modo de operación full-dúplex de los protocolos LAN (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring y FDDI). En este modo no hay etapa o fase de accesso al medio compartido y la velocidad de transmisión de datos se duplica.
- En el modo full-dúplex las sobrecargas del switch se previenen al utilizar el método de retroalimentación descrito en el estándar 802.3x. Esto suspende temporalmente la transmisión de la trama desde los vecinos más cercanos al switch sobrecargado.
- En el modo half-dúplex de operación del switch, los switches emplean dos métodos para controlar el flujo de tramas: captura agresiva del medio y presión hacia atrás sobre el nodo terminal. El uso de estos métodos permite un control de flujo suficientemente flexible para intercalar varias tramas transmitidas con una trama recibida.
- Las características principales del rendimiento del switch son la velocidad de filtrado de trama, la velocidad de direccionamiento de la trama, el rendimiento de todos los puertos en megabits por segundo y el retardo de transmisión de la trama.
- Las características del rendimiento del switch dependen del tipo de conmutación: al vuelo o con almacenamiento temporal completo, del tamaño de la tabla de dirección y del tamaño del búfer o memoria temporal de la trama.

- Los switches podrán filtrar el tráfico que se transmite de acuerdo con varios criterios, que toman en cuenta las direcciones fuente y de destino, además de los valores de campos arbitrarios. Sin embargo, el método de especificar filtros definidos por el usuario en la capa de enlace de datos es bastante complicado. Para dominar este método, el administrador debe conocer bien los protocolos y realizar la mayoría de las tareas difíciles para determinar la ubicación del atributo requerido dentro de la trama.

PREGUNTAS DE REPASO

1. Enumere las principales limitaciones de las redes basadas en un medio compartido.
2. ¿Por qué en las redes Ethernet el incremento brusco de retardos comienza en valores inferiores del coeficiente de uso del medio en comparación con los valores para las redes Token Ring y FDDI?
3. ¿Cuáles son las ventajas de los switches de LAN?
4. Una tabla de direccionamiento de switch se crea con base en:
   a) Direcciones fuente o de inicio.
   b) Direcciones de destino.
5. ¿Es posible establecer que cuando se divide un medio compartido en dos segmentos, la carga de cada segmento disminuye a la mitad?
6. ¿Cuáles son las consecuencias negativas de la presencia de ciclos o loops cerrados en una red creada con base en switches que funcionan de acuerdo con el algoritmo de puente transparente?
7. ¿Cuál es el objetivo de limitar el tiempo de vida de las entradas de la tabla de direccionamiento?
8. Compare los algoritmos de puente transparente y SRB.
9. ¿Cuáles son los propósitos de los filtros definidos por el usuario en los switches?
10. ¿Qué parámetros pueden utilizarse cuando se crea un filtro de un switch definido por el usuario?
11. ¿Puede exceder la velocidad de direccionamiento a la velocidad de filtrado?
12. ¿Qué es un switch sin bloqueo?
13. ¿Es posible para un switch sin bloqueo perder paquetes debido a sobreflujo?
14. ¿Qué mecanismos emplean los switches en condiciones de sobreflujo de cola interna?
    - Formato del tráfico.
    - Retroalimentación según la trama PAUSE.
    - Presión hacia atrás (colisiones artificiales).
    - Priorización.
15. ¿Puede la tecnología Ethernet 10G usar un medio compartido?
16. ¿Qué característica de la interfaz física corresponde al número 4 en el nombre de la especificación 10GBase-LX4?
17. ¿Es posible conectar de manera directa un switch de LAN con la interfaz 10GBase-WL al puerto STM-64 del multiplexor SDH?
18. ¿Qué propiedad de las tecnologías LAN simplifica la traducción de los protocolos Ethernet, Token Ring y FDDI?
19. ¿En qué casos puede la trama FDDI no ser traducida a la trama Ethernet?
20. Especifique los tipos principales de matriz de conmutación.

21. ¿Cuál es la principal desventaja de la matriz de conmutación?
22. ¿Cuál ventaja adicional está relacionada con el uso de la memoria compartida como una matriz de conmutación?
23. ¿Por qué la conmutación al vuelo tiene aplicación limitada en switches?
24. ¿Qué ocurre si el número de direcciones de LAN excede el tamaño de la tabla de dirección del switch?

PROBLEMAS

1. El filtro definido por el usuario incluye una condición lógica y la acción que debe realizarse sobre la trama en caso de que esta condición se satisfaga. Formule las condiciones del filtro que descarta las tramas que llegan desde la computadora A, que tiene la dirección MAC 06 DB 00 34 5E 27, y desde la computadora B, que tiene la dirección MAC CC 33 00 D5 43 4D, hacia el servidor S, cuya dirección MAC es CC 33 00 65 44 AA.

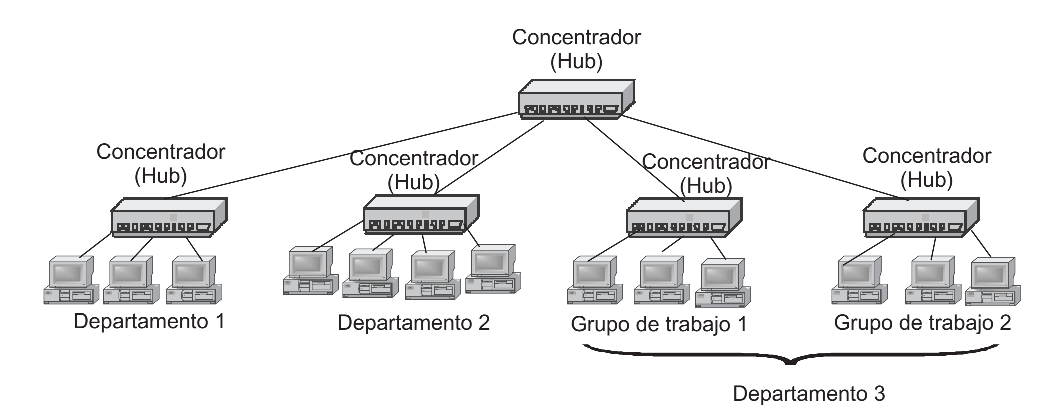


FIGURA 15.25 Red que se actualizará.

2. Es necesario mejorar el rendimiento de una red basada en un medio compartido (figura 15.25). Sólo cuenta con un switch a su disposición; tiene dos puertos de 1 000 Mbps y ocho puertos de 100 Mbps. ¿Cómo transformaría la red, si es posible, para continuar empleando los concentradores (hubs) disponibles en la variante inicial?

16 CARACTERÍSTICAS AVANZADAS DE LAN CONMUTADAS

DESCRIPCIÓN DEL CAPÍTULO

16.1 INTRODUCCIÓN

Los switches permiten construir redes significativamente más grandes al dividir un medio compartido en partes o al abandonar el principio de la repartición del medio a favor de LAN conmutadas. No obstante, a medida que se incrementa la escala de la red, surgen otros problemas que no puede superar el switch basado sólo en el algoritmo de puente transparente considerado en el capítulo anterior. En primer lugar, el problema de confiabilidad permanece sin resolver, pues la topología de árbol de las LAN conmutadas es extremadamente vulnerable. Por ejemplo, la falla de cualquier switch o enlace de comunicaciones produce una pérdida de conectividad. Si el switch del segmento falla, la red se dividirá en dos o más segmentos.

Las limitaciones de la topología de árbol pueden evitarse si se usan mecanismos adicionales de conmutación mismos que proporcionan características avanzadas a las LAN. Por ejemplo, el algoritmo de árbol de expansión (STA, por sus siglas para Spanning Tree Algorithm) se utiliza con gran amplitud en LAN conmutadas. STA se desarrolló de manera simultánea con el algoritmo de puente transparente (es decir, a principios de la década de 1980) y desde entonces se ha empleado con éxito en LAN.

Otro mecanismo del uso de rutas alternativas se desarrolló comparativamente de manera reciente, cuando comenzó el uso extendido de las LAN conmutadas. El mecanismo de agregación de enlace permite a varios enlaces físicos unirse en un canal lógico, lo cual mejora el rendimiento de la red y su confiabilidad.

Las nuevas capacidades avanzadas de los switches de LAN facilitan poner en práctica diversos mecanismos comunes de soporte de calidad de servicio (QoS) que puedan implementarse, dirigidos a diferentes clases de tráfico: colas ponderadas y de prioridad, retroalimentación y reservación de recursos.

A pesar del progreso conseguido con el uso de nuevas características agregadas por el STA y el mecanismo de agregación de enlace, las LAN construidas solamente con base en switches, sin utilizar enrutadores, se caracterizan por algunas limitaciones y experimentan ciertos problemas. Es posible resolver parte de ellos si se aplica una importante propiedad avanzada de una LAN conmutada: la técnica de LAN virtual (VLAN, por sus siglas en inglés), que simplifica de modo considerable el empleo de enrutadores en tales redes. La técnica de VLAN permite que una LAN se divida en varios segmentos lógicos aislados. Esto se consigue mediante la configuración de switch (es decir, de manera programática más que físicamente, mediante la conexión o desconexión de enchufes de cable). Estos segmentos aislados pueden conectarse entonces en la red interna, para lo cual se utiliza el protocolo de capa de red. La división programática de una red en segmentos favorece cambios de manera rápida y fácil a la composición de los segmentos al mover computadoras de segmento a segmento en la medida en que sea necesario.

16.2 ALGORITMO DE ÁRBOL DE EXPANSIÓN

PALABRAS CLAVE: algoritmo de árbol de expansión (STA, Spanning Tree Algorithm), protocolo de árbol de expansión (STP, Spanning Tree Protocol), segmento, switch raíz, métrica, identificador de switch, puerto raíz, identificador de puerto, puerto designado, unidad de datos de protocolo de puente (BPDU, Bridge Protocol Data Unit) e intervalo "hello".

En aquellas LAN donde tanto las tecnologías como el equipo ponen en marcha las funciones de únicamente la primera y la segunda etapas del modelo ISO/OSI, el problema de utilizar

rutas alternativas tiene sus propias características específicas: los protocolos base soportan sólo *topologías tipo árbol* (es decir, aquellas que no contienen ningún ciclo o loop).

Para conmutación automática dentro de un estado reservado de todos los enlaces alternativos que no se ubican en el esquema de la topología de árbol, las LAN utilizan el **algoritmo de árbol de expansión (STA)**. El protocolo que implementa este algoritmo se denomina **protocolo de árbol de expansión (STP)**.

STA fue diseñado hace bastante tiempo, en 1983. El IEEE lo adoptó y se incluyó en la especificación 802.1D, que describía el algoritmo de puente transparente. Aunque los puentes para los cuales este algoritmo fue destinado en un principio se consideran dispositivos de comunicación "de la edad de las cavernas", STA se usa ampliamente en la mayoría de dispositivos de comunicaciones generalizados en las LAN contemporáneas: en switches. STA facilitó a los diseñadores de redes construir LAN a gran escala con base en switches sin utilizar enrutadores. Tales LAN están caracterizadas por su alta confiabilidad debido al empleo de enlaces de reserva.

Como regla, los fabricantes de equipo de red instalan STA en switches dirigidos a segmentos de red caracterizados por requerimientos crecientes de confiabilidad, como switches troncales y switches de departamentos de grandes grupos de trabajo.

16.2.1 Definiciones requeridas

STA representa la red en forma de una gráfica cuyos nodos son switches y segmentos de red (figura 16.1).

Un **segmento** es una parte conectada de una red que no contiene switches o enrutadores. Puede ser compartido (cuando se diseñó STA, éste era el único tipo de segmento) e incluir dispositivos de capa física como repetidores o concentradores, los cuales son transparentes para el switch. En la actualidad, el segmento suele ser un enlace dúplex punto a punto entre los puertos adyacentes de dos switches.

STA asegura la construcción de una topología de árbol de enlaces con solamente una trayectoria de longitud mínima desde cada switch y cada segmento hacia algún **switch raíz** dedicado: la raíz del árbol. La *unicidad* de la trayectoria asegura que se esté libre de ciclos o loops y lo *mínimo* de la distancia permite construir una trayectoria óptima para el tráfico de viaje de la periferia de la red hacia su línea central o troncal, papel que es representado por el switch raíz.

Como una medida de la distancia, STA usa la **métrica** tradicional para protocolos de enrutamiento: el valor inversamente proporcional al ancho de banda del segmento. En STA, la métrica también está definida como el costo designado del segmento. Se calcula como el tiempo requerido para transmitir 1 bit de información y se mide en unidades de 10 nseg (nanosegundos). De este modo, para el segmento Ethernet de 10 Mbps, el costo designado es de 10 unidades condicionales; para Ethernet de 100 Mbps, es de 1 unidad y para el segmento Token Ring de 16 Mbps, valor que es de 6.25. Dado que la velocidad de la red se encuentra en crecimiento constante, ha aparecido una versión modificada y revisada de la escala de unidad condicional: 10 Mbps: 100, 100 Mbps: 19, 1 Gbps: 4 y 10 Gbps: 2.

El **identificador de switch** es el número de 8 bytes, cuyos seis bytes menos significativos contienen la dirección MAC de la unidad de control del switch que implementa STA. Recuérdese que los puertos de los switches y puentes no requieren direcciones MAC para llevar a cabo su función principal, de modo que sólo es una dirección MAC del puerto. Los dos bytes más significativos del identificador de switch son configurados de forma manual. Como se verá más adelante, esto permite al administrador de la red influir en el proceso de selección del switch raíz.

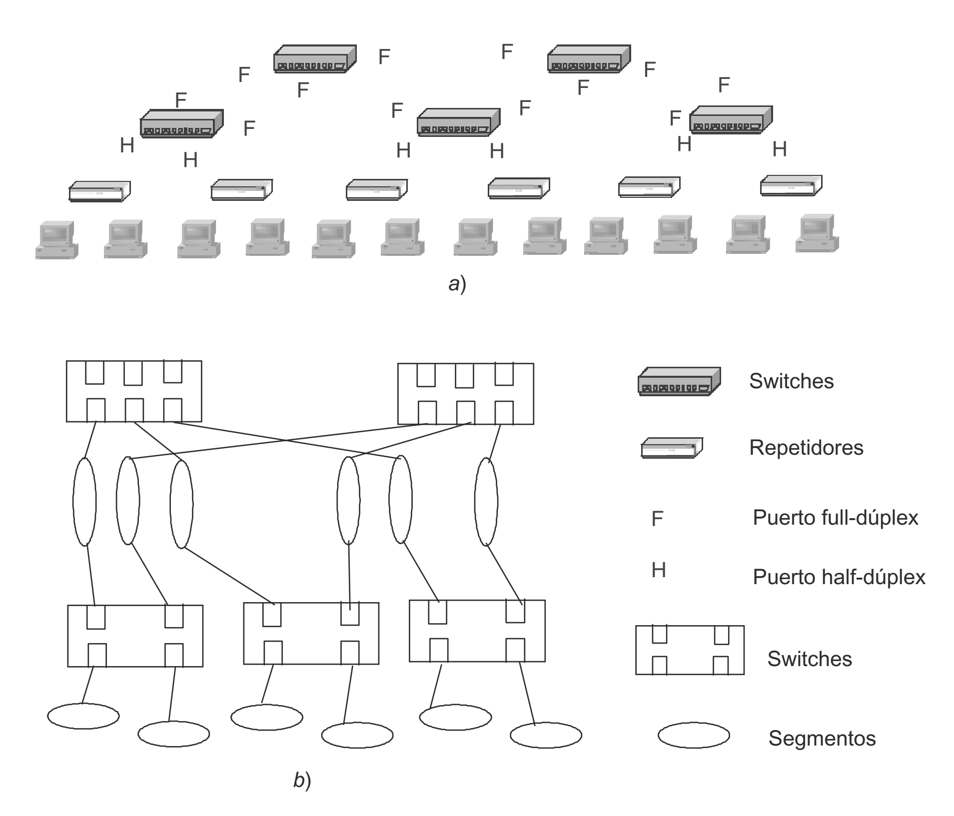


FIGURA 16.1 Representación formal de la red de acuerdo con STA**.**

El **puerto raíz** del switch es aquel que tiene la distancia más corta desde el switch raíz (con más precisión, desde cualquiera de los puertos del switch raíz).

El **identificador de puerto** es un número de 2 bytes. El byte menos significativo contiene el número ordinal de este puerto dentro de un switch, mientras que el más significativo lo establece de forma manual el administrador de la red.

El **puerto designado** es la distancia más corta desde el switch raíz entre todos los puertos de todos los switches de este segmento.

El **switch designado** del segmento es aquel switch al que pertenece el puerto designado de este segmento.

Las **unidades de datos del protocolo del puente (BPDU)** son paquetes especiales con los que los switches intercambian automáticamente para detección automática de la configuración del árbol. Las BPDU conducen datos acerca de los identificadores del puerto y el switch e información acerca del costo de trayectoria desde el switch raíz. En STA, el intervalo en el que son generados los paquetes BPDU se conoce como *intervalo hello,* el cual es fijado por el administrador y por lo regular abarca desde 1 a 4 segundos.

16.2.2 Procedimiento de tres etapas para construcción del árbol

La figura 16.2 suministra la red de ejemplo que se utilizará para ilustrar el procedimiento de construcción de un árbol de expansión.

STA determina la configuración activa de la red en tres etapas.

Etapa 1. Se selecciona el switch raíz desde el cual se construirá el árbol. De acuerdo con STA, este papel es delegado al switch que tiene el *valor de identificador más pequeño.* Si el administrador de la red no interfiere con este proceso, el switch raíz se elegirá de manera aleatoria. De hecho, el dispositivo que tiene el valor mínimo de la dirección MAC de la unidad de control será el elegido para este papel. Como es natural, esta selección difícilmente puede ser óptima. Por ejemplo, si el switch 5 es elegido para ser el switch raíz (figura 16.2), la mayor parte del tráfico pasará a través de muchos switches y segmentos de tránsito. Por lo tanto, el administrador de la red no debería permitir que este proceso continúe su curso. Sería mucho mejor si el administrador pudiera influir en este proceso y elegir el switch raíz con base en consideraciones razonables. Esto se logra al establecer una configuración apropiada de los bytes más significativos en los identificadores del switch. Si se procede de tal manera, será posible seleccionar el switch que tome la posición central en las conexiones entre segmentos. Suponga que los identificadores del switch corresponden a los números mostrados en la ilustración. En este caso, se debe seleccionar el switch 1 para el papel de raíz.

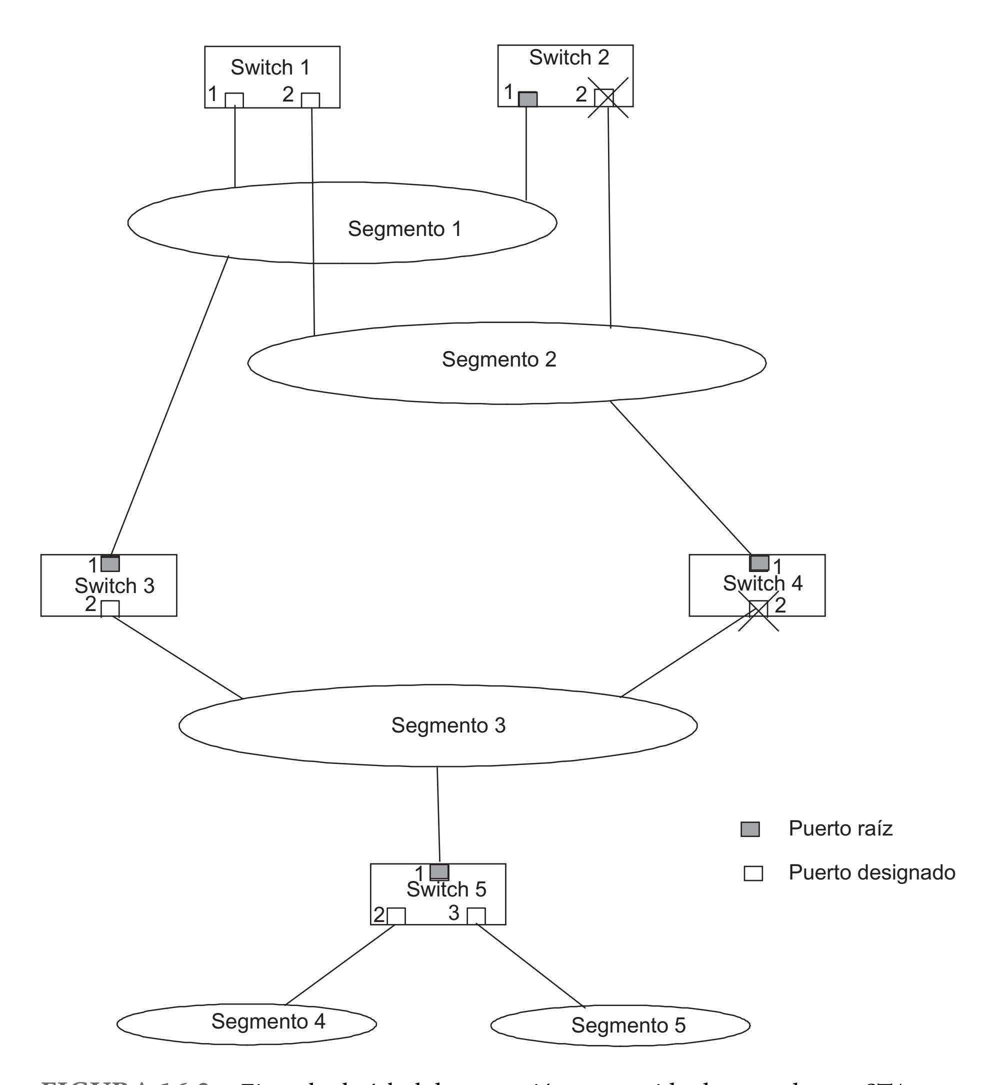


FIGURA 16.2 Ejemplo de árbol de expansión construido de acuerdo con STA.

Etapa 2. Se selecciona el puerto raíz para cada switch. La distancia desde el switch raíz está determinada por los BPDU que llegan desde este switch. Según los datos de estos paquetes, cada switch puede determinar las distancias mínimas desde el switch raíz hacia todos los puertos. Cada switch analiza el BPDU recibido, incrementa el costo de trayectoria desde el switch raíz especificado en ese BPDU por el costo designado del segmento desde el cual fue recibido ese paquete y entonces vuelve a transmitir el BPDU. Así, la distancia desde el switch raíz especificado en una BPDU se incrementa a medida que pasa a través de los switches. Por ejemplo, suponiendo que todos los segmentos en el ejemplo considerado son segmentos Ethernet 10 Mbps, el switch 2, una vez que ha recibido un BPDU con la distancia establecida a 0 desde el segmento 1, lo incrementará en 10 unidades condicionales.

Cuando se vuelven a traducir los paquetes, cada switch "memoriza" la distancia mínima desde la raíz encontrada en todos los BPDU recibidos por cada uno de sus puertos. Cuando se ha definido la configuración del árbol de expansión, cada switch encuentra su puerto raíz (es decir, el que tiene la distancia mínima desde la raíz).

Si los valores métricos son iguales, los identificadores del switch y el puerto se utilizarán para eliminar la ambigüedad. Se da preferencia a los puertos y switches con valores de identificador mínimo. Por ejemplo, para el segmento 3 existen dos trayectorias hacia el switch raíz 1, ambas con valores iguales de la métrica. La primera trayectoria pasa a través del switch 3, mientras que la segunda viaja a través del switch 4. La trayectoria seleccionada pasa a través del switch que tiene el *valor de identificador más pequeño* (es decir, a través del switch 3). En este caso, coinciden los números de puerto dentro de los switches; sin embargo, cuando se lleva a cabo la comparación, el *identificador de switch* se considera antes que el número de puerto.

En el ejemplo mostrado en la figura 16.2, el switch 3 selecciona el puerto 1 como su puerto raíz, ya que para este puerto la distancia mínima desde la raíz es de 10 unidades (un BPDU con una distancia así fue recibido desde el switch raíz a través del segmento 1). El puerto 2 del switch 3, con base en los paquetes recibidos, ha determinado que la distancia mínima desde la raíz es de 20 unidades. Esto corresponde a cuando el paquete pasa desde el puerto 2 del switch raíz por el segmento 2 y luego pasa a través del switch 4 y el segmento 3. El switch 2, cuando selecciona el puerto raíz, ha encontrado la situación en la cual sus puertos 1 y 2 se encuentran a igual distancia de la raíz: 10 unidades. El puerto 1 recibe los paquetes desde el puerto 1 del switch raíz a través de un segmento de tránsito, el segmento 1, mientras que el puerto 2 recibe paquetes desde el puerto 2 del switch raíz a través del segmento 2. Como el valor numérico del identificador del puerto 1 es más pequeño que el correspondiente al puerto 2, el puerto 1 será elegido como el puerto raíz.

Etapa 3. El puerto designado es elegido de entre todos los puertos de todos los switches dentro de los límites de un segmento de red y el switch correspondiente a ese puerto se convierte en el switch designado de ese segmento. De manera semejante a la selección del puerto raíz, se aplica aquí el procedimiento distribuido. Cada switch del primer segmento excluye de la consideración su puerto raíz debido a que, para el segmento al que ese puerto está conectado, siempre hay otro switch más cercano a la raíz. Para todos los puertos restantes, sus distancias mínimas desde el switch raíz (antes de incrementarlo por el tiempo convencional del segmento) se comparan con la distancia desde la raíz obtenida para el puerto raíz de este switch. Si todas las distancias recibidas en ese puerto son más grandes que la determinada para el puerto raíz del switch para el segmento al cual ese puerto está conectado, la trayectoria más corta hacia el switch raíz pasará a través de este switch. En consecuencia, este switch se convierte en uno designado. El switch convierte todos sus puertos para los cuales se satisface esta condición en puertos designados. Donde existen varios puertos con la misma distancia más corta desde el switch raíz, se elige el puerto con el identificador más pequeño.

En el ejemplo considerado, el switch 2 ha detectado que los paquetes con la distancia más corta, 0 unidades, fueron recibidos a través del puerto 2 (éstos fueron paquetes desde el puerto 2 del switch raíz 1). Dado que para el puerto raíz del switch 2 la distancia desde la raíz es 10, el puerto 2 de este switch no es un puerto designado para el segmento 2.

De manera predeterminada, los switches de la red tienen 15 segundos para completar las tres etapas. Se supone que durante este tiempo cada switch recibe un número suficiente de BPDU, lo cual le permite determinar el estado de todos sus puertos.

Los otros puertos, excepto los puertos raíz y los designados, se conmutan al estado de bloqueo (en la ilustración, tales puertos están tachados) y se completa el procedimiento de construcción del árbol de expansión. Se ha probado matemáticamente que este método para seleccionar puertos activos elimina los ciclos o loops en la red y que las conexiones restantes forman un *árbol de expansión* (siempre que pueda crearse con los enlaces de red existentes).

NOTA *En general, la topología de árbol elegida de acuerdo con STA no es la óptima para todas las trayectorias posibles de transmisión de tráfico. Como vemos, en el ejemplo propuesto, el tráfico pasa a través de la trayectoria siguiente cuando se transmiten paquetes desde el segmento 3 hacia el segmento 2: switch 3 – segmento 1 – switch 1 – segmento 2. La métrica para esta trayectoria es 30. Si el puerto 2 del switch 4 no fue bloqueado, habría una trayectoria más corta: la que va a través del switch 4. La métrica de esta trayectoria sería 20, que es mejor que la trayectoria anterior.*

Una variante así será posible si la trayectoria más corta hacia el switch raíz para el segmento 4 es elegida a través del switch 4 en vez del switch 3. Esto puede conseguirse al asignar de manera apropiada los valores para las partes más significativas de los identificadores del switch. Sin embargo, si se elige esta variante, la trayectoria más corta desde el segmento 4 hasta el segmento 1 no será la trayectoria óptima.

Una vez diseñado el árbol de expansión, el switch comienza a recibir (sin direccionamiento) agentes de datos y a construir la tabla de direccionamiento con base en sus direcciones fuente o de origen. Éste es un modo de aprendizaje de puente transparente normal que podría no ser activado antes, pues el puerto no estaba seguro si permanecía como raíz o se convertía en un puerto designado que transmitiría paquetes de datos. La etapa de "aprendizaje" también dura 15 segundos de manera predeterminada. Al mismo tiempo, el puerto continúa con su participación en la operación del STA, lo cual significa que la llegada de una BPDU con mejores parámetros automáticamente la conmutará en el estado "bloqueado".

Sólo después de que transcurre un espacio de tiempo del doble de duración que el valor predefinido de descanso, el puerto conmuta al estado de direccionamiento y comienza a procesar paquetes de acuerdo con la tabla de direccionamiento que ha generado. Nótese que esta tabla continúa siendo modificada y refleja los cambios en la estructura de la red.

En el transcurso del funcionamiento normal, el switch aún genera BPDU de configuración en el intervalo hello; otros switches los reciben a través de sus puertos raíz y vuelven a traducirlos por medio de los puertos designados. El switch puede carecer de puertos designados (por ejemplo, los switches 2 y 4); no obstante, participa en la operación del protocolo STA, debido a que el puerto raíz continúa recibiendo paquetes BPDU.

Si el puerto raíz de cualquier switch de red no recibe un BPDU después de transcurrir el máximo **tiempo de vida (TTL**, por sus siglas para **Time To Live)** de un mensaje (20 segundos predeterminados), inicia un nuevo procedimiento de construcción del árbol de expansión. En este caso, el switch genera una BPDU donde se especifica como una raíz y traduce esto a todos los switches. Los otros switches de la red con el temporizador TTL del mensaje expirado proceden de manera similar; como resultado, se elige una nueva configuración activa.

16.2.3 Ventajas y desventajas del STA

Una de las principales ventajas del STA es que, en contraste con la mayoría de otros algoritmos simplificados donde la conexión reservada entra en funciones exclusivamente cuando el dispositivo vecino falla, éste realiza la reconfiguración de la red no solamente con el conteo de los enlaces a sus vecinos más cercanos, sino también con el conteo del estado de los enlaces en segmentos distantes de la red.

Las desventajas de este algoritmo incluyen que en redes con numerosos switches, el tiempo requerido para determinar una nueva configuración activa puede ser demasiado largo. Si la red utiliza valores de descanso predeterminados, la transición a una nueva configuración puede tomar más de 50 segundos. Se requieren 20 segundos para confirmar la pérdida de conectividad con el switch raíz (la expiración del temporizador es la única forma de obtener información acerca de este evento en la variante estándar del STA) y se necesitarán 2×15 segundos adicionales para entrar al estado de "direccionamiento".

Las versiones existentes no estándar del STA, que son bastante numerosas, permiten que el tiempo de reconfiguración se reduzca mediante una complicación adicional del algoritmo. Esto puede conseguirse al agregar nuevos tipos de mensaje de control. En 2001 se diseñó una nueva versión del árbol de expansión: la especificación IEEE 802.1w, también dirigida a acelerar la operación del protocolo, pero de una manera estándar.

16.3 AGREGACIÓN DE ENLACE EN LAN

PALABRAS CLAVE: agregación de enlace, troncal, eliminación de generación de tramas, selección de puerto, puerto lógico, puertos físicos, distribución dinámica y estática de tramas, protocolo de agregación de control de enlace (LCAP, Link Control Aggregation Protocol) e IEEE 802.3ad.

16.3.1 Canales lógicos y troncales

La **agregación de enlace** entre los dispositivos de comunicaciones en un canal lógico simple es otra forma de utilizar enlaces alternativos redundantes en las LAN.

La diferencia principal entre la técnica de agregación de enlace y el STA previamente descrito es:

- STA conmuta los enlaces redundantes a reserva de última hora y deja en estado activo sólo el conjunto mínimo de canales requerido para asegurar la conectividad de los segmentos de la red. En este caso, se incrementa la *confiabilidad* de la red, pero su rendimiento se mantiene igual.
- Cuando se utiliza agregación de enlace, todos los enlaces redundantes permanecen activos, lo que mejora tanto la *confiabilidad* de la red como su *rendimiento*.

Si falla de uno de los componentes de un canal agregado de esta clase, a menudo denominado **troncal**, el tráfico se distribuirá entre los enlaces restantes (figura 16.3). En la ilustración, el ejemplo de una situación así es el troncal 2, en el cual uno de los enlaces (el central) ha fallado, de modo que todas las tramas se transmiten con los dos enlaces restantes. Este ejemplo ilustra el mejoramiento de la *confiabilidad*.

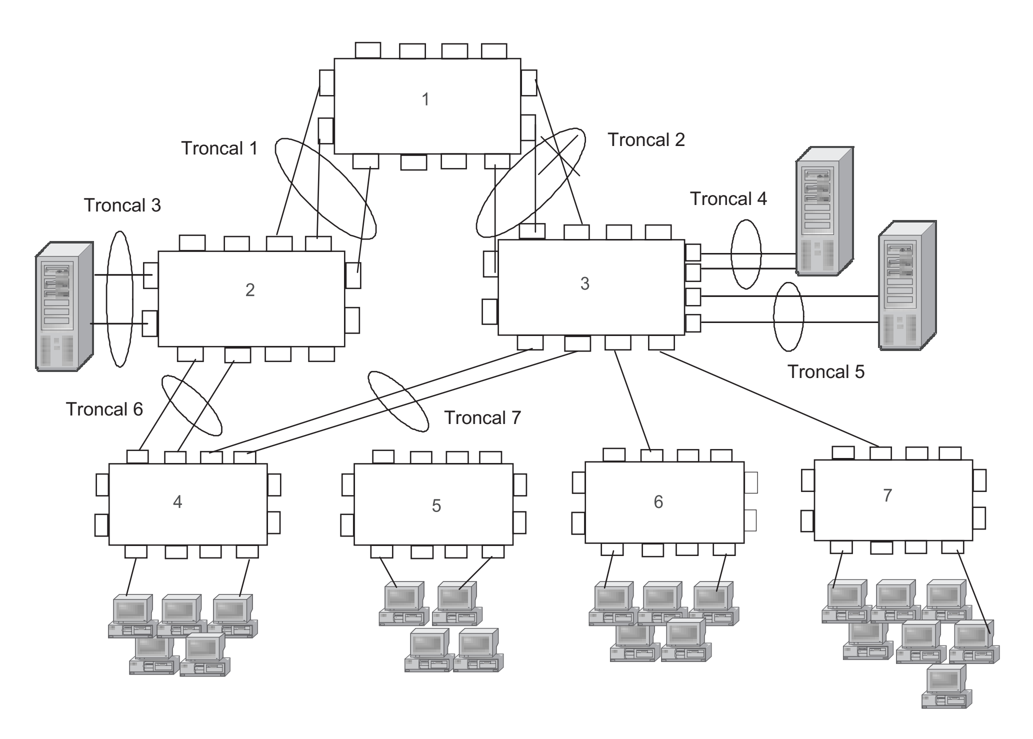


FIGURA 16.3 Agregación de enlaces físicos.

Ahora considérese la manera en que la agregación de enlaces mejora el *rendimiento* de la red. Por ejemplo, en la figura 16.3, los switches 1 y 3 están conectados mediante tres enlaces paralelos. Esto incrementa el rendimiento de esta sección al triple en comparación con la variante estándar de la topología de árbol, la cual no permite enlaces paralelos. La mejora del rendimiento de la conexión entre switches obtenida mediante la agregación de enlaces en algunos casos es más eficaz que la conseguida al reemplazar un enlace físico simple con uno más rápido. Por ejemplo, a pesar de la variedad de velocidades de enlace físico suministradas por la familia Ethernet (de 10 Mbps a 100 Gbps) un incremento de 10 veces la velocidad obtenida por la migración a un estándar Ethernet más rápido no siempre es necesario ni económicamente justificable. Por ejemplo, si los switches de redes instalados en la red no facilitan agregar un módulo equipado con el puerto Gigabit Ethernet, incrementar la velocidad hasta 1 000 Mbps en algunos enlaces requerirá un reemplazo total de switches. Por otra parte, los switches existentes pueden tener puertos Fast Ethernet libres. Por tanto, es posible incrementar la velocidad de los datos hasta 600 Mbps al agregar seis enlaces Fast Ethernet.

La agregación de enlace es una forma generalizada del tercer método para utilizar rutas alternativas descrito en el capítulo 6 ("La red encuentra dos rutas de antemano pero usa sólo una de ellas").[1] En este caso, en vez de dos rutas, se encuentran N rutas (donde $N \geq 2$) y solamente una de ellas se emplea para cada flujo. Cuando esta ruta falla, el flujo afectado por dicha falla es cambiado a cualquiera de las (N – 1) rutas que permanecen en operación.

[1] Véase la sección "Rutas alternativas".

La agregación de enlace se utiliza para los enlaces entre los puertos de dos switches de LAN, para enlaces entre computadoras y switches. Con más frecuencia, esta variante se pone en práctica para servidores rápidos o servidores críticos de negocios. En este caso, todos los adaptadores de red o puertos de switch que componen un troncal comparten las mismas direcciones de red. Debido a esto, los puertos troncales no son distinguibles para IP o para cualquier otro protocolo de capa de red, lo cual corresponde al concepto de un canal lógico unido y sirve como base para la agregación de enlace.

Casi todos los métodos de agregación de enlace utilizados hoy en día tienen una limitación significativa: toman en cuenta únicamente los enlaces entre dos switches de red vecinos, pero ignoran todo lo que tiene lugar fuera de los límites de su sección de la red. Por ejemplo, la operación del troncal 1 no está coordinada con la operación del troncal 2, y la presencia de un enlace normal entre los switches 2 y 3, que crea un ciclo o loop con los troncales 1 y 2, no es tomada en cuenta. Debido a ello, la delegación de enlace debe utilizarse *con* STA si el administrador de la red quiere emplear todas las capacidades topológicas de la conexión de los nodos de red. Para STA, el troncal debe parecer un enlace simple, en cuyo caso la operación lógica del STA entrará en vigor.

Existen muchas implementaciones que tienen el mecanismo de agregación de enlace. Naturalmente, las más populares pertenecen a los líderes en el campo de la industria de los equipos de LAN. Esta lista incluye implementaciones tan conocidas como Fast EtherChannel y Gigabit EtherChannel de Cisco, MultiLink Trunking de Nortel y Adaptative Load Balancing (equilibrio de carga adaptativa) de Intel. El IEEE 802.3ad (agregación de enlace) resume y generaliza estos enfoques.

16.3.2 Eliminación de la generación de tramas

Ahora considérense con más detalle las características específicas del funcionamiento de switches cuando sus puertos componen un troncal. En el fragmento de la red mostrado en la figura 16.4, los switches 1 y 2 están conectados mediante cuatro enlaces físicos. Advierta que un troncal puede ser unidireccional o bidireccional. Cada switch controla solamente el envío de tramas y decide cuál será el puerto de salida al que debe transmitirse. Por lo tanto, si ambos switches consideran los enlaces que los conectan como un troncal, éste será bidireccional; de otro modo, será un troncal unidireccional.

La figura 16.4 muestra el comportamiento del switch 1 en relación con enlaces paralelos. Si estos enlaces no son considerados por un switch como un enlace agregado, habrá problemas con dos tipos de tramas:

- Tramas que llevan direcciones únicas *no aprendidas* por el switch.
- Tramas que conducen una dirección de *difusión* o *multidirigida.*

El algoritmo de puente transparente requiere que el switch transmita una trama con una dirección no aprendida u olvidada (es decir, desaparecida u olvidada de la tabla de direccionamiento) a todos los puertos, excepto aquel desde el cual se recibió esa trama. Si existen enlaces paralelos, se generará una trama de ese tipo y el número de sus copias será igual a la cantidad de enlaces paralelos. En el ejemplo suministrado, el switch 2 recibiría cuatro copias de la trama original.

Al mismo tiempo, las tramas caerían en un ciclo infinito porque circularían constantemente entre dos switches. Nótese que tales tramas no pueden eliminarse en la red, pues los protocolos de la capa de enlace de datos a menudo carecen del campo *TTL*, utilizado a menudo en protocolos de capa superior tales como IP o IPX.

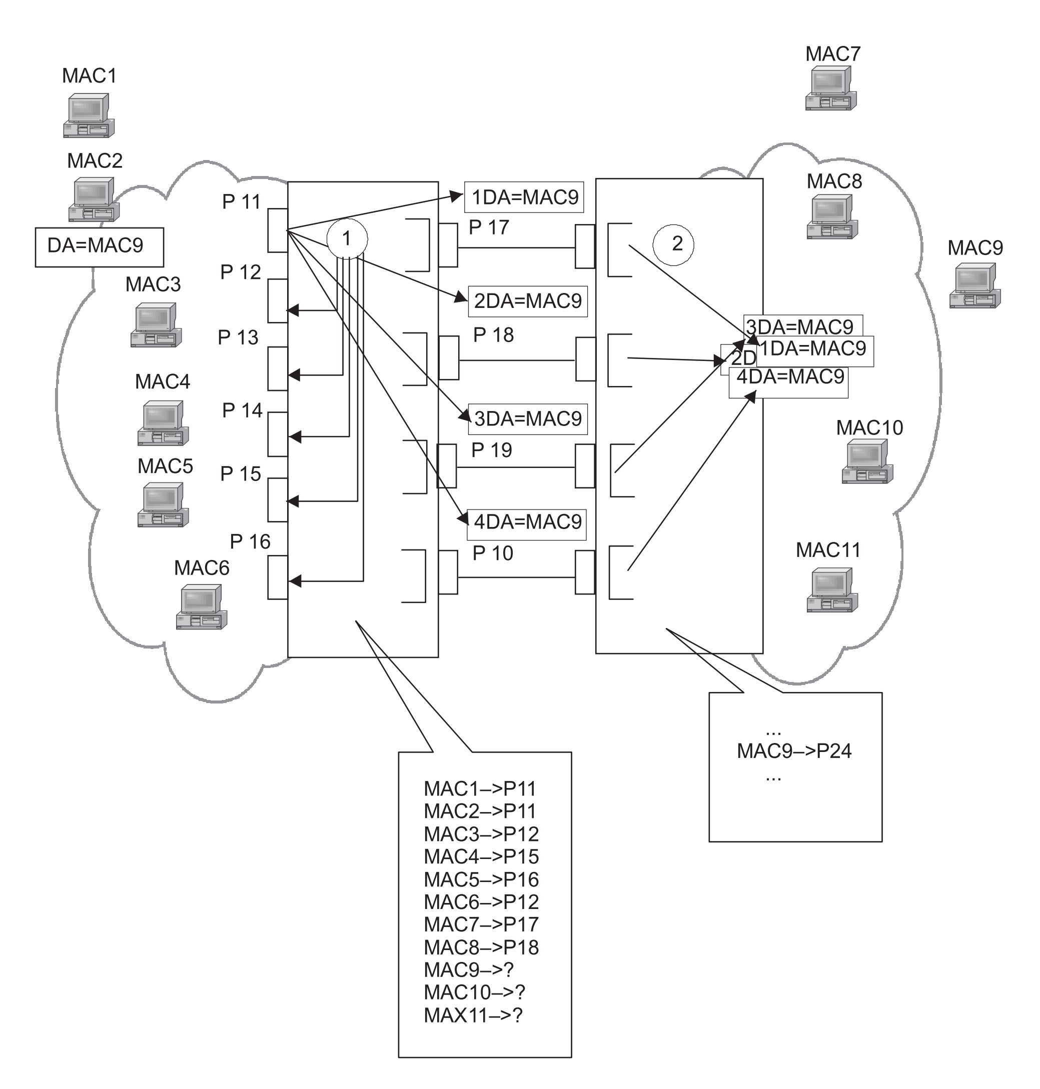


FIGURA 16.4 Generación de paquetes con una dirección olvidada cuando se utilizan enlaces paralelos entre switches.

En cualquier caso, la trama con la dirección olvidada aumentaría la carga de la red al incrementar el número de tramas. Esto probablemente produciría bloqueos, retardos y pérdidas de datos. Aparte del aumento de la carga de la red, la duplicación de tramas también produciría la operación ineficaz de muchos protocolos de capa superior. Considérese, por ejemplo, el nodo ejecutando TCP, que utiliza duplicación ACK como una señal indirecta de la congestión de la red.

Las tramas que contienen direcciones de difusión crean aún más problemas porque deben transmitirse a todos los puertos con excepción del puerto de origen. De este modo, la red llegará a inundarse con tráfico irrelevante, esta carga será más significativa y las tramas caerán en ciclos infinitos.

Los problemas con tramas conocidas y direcciones de destino único no se presentan. Esto se debe a que el switch transmite tales tramas a un puerto simple: aquel a través del cual ha llegado la trama con esa dirección en el campo de dirección de origen.

Los diseñadores de mecanismos de agregación han tomado en cuenta los problemas que surgen cuando se procesan tramas con direcciones olvidadas, de difusión o multidirigidas. La solución a este problema es simple: implica que todos los puertos conectados por enlaces paralelos sean considerados un solo *puerto lógico*, especificado en la tabla de direccionamiento, en lugar de varios *puertos físicos*. En la figura 16.4, la tabla de direccionamiento contiene un solo puerto lógico, AL11, en vez de los puertos P17, P18, P19 y P10. Las direcciones de todos los nodos, cuyas trayectorias pasan a través del switch 2, están mapeadas a este puerto. Al mismo tiempo, el aprendizaje de una nueva dirección conducida por la trama que llega desde cualquiera de los puertos físicos incluidos en el troncal inserta una nueva entrada en la tabla de direccionamiento. Esta nueva entrada contendrá el identificador del puerto lógico. La trama que llega, cuya dirección de destino es aprendida y mapeada para el identificador del puerto lógico, se transmite hacia únicamente un puerto de salida del switch, el cual está incluido en el troncal. El switch procesa las direcciones olvidadas, de difusión o multidirigidas de la misma manera: utiliza sólo uno de los enlaces para la transmisión de la trama. Este cambio en la lógica de procesamiento de la trama no se aplica a los puertos del switch que no están incluidos en el troncal. Por ejemplo, el switch 1 siempre transmite tramas con direcciones olvidadas o de difusión hacia los puertos P11-P16.

Debido a esta decisión, las tramas no se duplican y el problema descrito con anterioridad no se presenta.

NOTA *De hecho, esto es correcto sólo si ambos switches consideran los enlaces paralelos como un troncal. De este modo, para usar completamente las propiedades troncales, es necesario configurarlas en ambos sentidos.*

16.3.3 Selección del puerto

Queda abierta una cuestión: ¿cuál de los puertos del switch tiene que utilizarse para el direccionamiento de la trama a través de un troncal?

Se pueden sugerir diversas variantes de una respuesta. El mejoramiento del rendimiento total de la sección de red entre dos switches o entre un switch y un servidor es uno de los objetivos de la agregación de enlace. Debido a ello, es deseable asegurar la **distribución dinámica de la trama** sobre los puertos del troncal, con base en la carga actual de cada puerto. Esto significa que las tramas recién llegadas se envían a los puertos con menores cargas (por ejemplo, con colas de espera más cortas). Parece que el método dinámico de distribución de tramas, que toma en cuenta la carga actual de cada puerto y asegura el equilibrio de la carga sobre todos los enlaces del troncal debe producir el rendimiento máximo del troncal completo.

Sin embargo, esta afirmación no siempre es verdadera, pues no explica el comportamiento de los protocolos de la capa superior. Existen algunos protocolos cuyo rendimiento se podrá ver significativamente reducido si los paquetes de la sesión establecida entre dos nodos terminales llegan en orden diferente del cual fueron enviados por el nodo fuente o de origen. Una situación así podrá ocurrir si dos o más tramas secuenciales de la misma sesión son transmitidas por puertos diferentes del troncal, porque las colas en los búferes de estos puertos tienen longitudes distintas. En consecuencia, los retardos de transmisión de la trama también pueden ser diversos, de modo que una trama transmitida posteriormente llegará al nodo de destino antes que una transmitida con anterioridad.

De lo anterior se infiere que la mayoría de los mecanismos de agregación de enlace utilizan métodos de **distribución estática de las tramas** entre los puertos en lugar de métodos de distribución dinámica. La distribución estática supone que un puerto específico del troncal

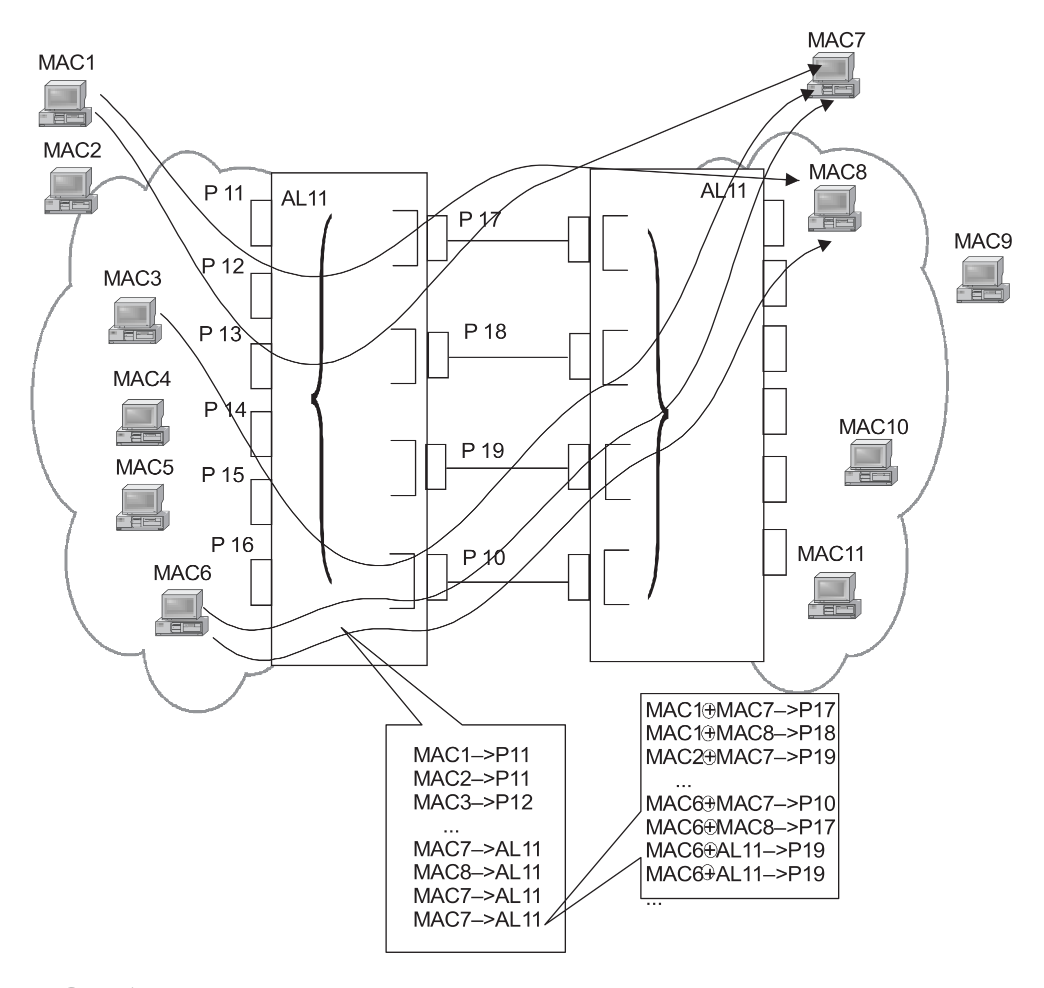


FIGURA 16.5 Red que utiliza el mecanismo Fast EtherChannel.

está asignado para el flujo de tramas de cierta sesión establecida entre dos nodos. Todas las tramas de esa sesión pasarán a través de la misma cola, lo cual asegura que llegarán al nodo de destino en el mismo orden en que fueron enviadas.

Por lo regular, cuando se emplea distribución estática, se selecciona el puerto para una sesión específica con base en ciertos atributos de los paquetes que llegan. Las direcciones MAC de origen o de destino o incluso ambas suelen emplearse como tales atributos. En la popular implementación Fast EtherChannel de Cisco (los switches pertenecientes a la familia Catalyst 5 000/6 000), se utiliza una operación de OR exclusivo (XOR) sobre los últimos dos bits de las direcciones MAC de origen y de destino para seleccionar el número de puerto troncal. El resultado de esta operación puede tomar uno de cuatro valores: 00, 01, 10 u 11, que son los números convencionales de los puertos troncales. La figura 16.5 muestra un ejemplo de una red en la que se usa el mecanismo Fast EtherChannel. La distribución de flujos para las sesiones entre nodos terminales es aleatoria en este caso. Como esta distribución no explica la carga real creada por cada sesión, el ancho de banda total del troncal puede usarse de manera ineficaz, en especial si las intensidades de la sesión son significativamente distintas. Además, este algoritmo no garantiza incluso la distribución uniforme a nivel cuantitativo de las sesiones sobre los puertos. El conjunto aleatorio de las direcciones MAC

en la red puede hacer que uno de los puertos transmita decenas de sesiones, mientras que otro puerto transmita sólo dos o tres sesiones. Cuando se utiliza este algoritmo, el equilibrio de carga para los puertos puede conseguirse solamente si se establecen muchas sesiones y computadoras en red entre ellas.

También pueden sugerirse otros métodos para distribuir sesiones entre los puertos. Por ejemplo, esta tarea puede realizarse de acuerdo con las direcciones IP de los paquetes encapsulada en las tramas de la capa de enlace de datos, o los tipos de protocolos de la capa de aplicación. Por ejemplo, se podrá transmitir el correo electrónico (e-mail) si se utiliza un puerto, el tráfico de Internet (web) si se emplea otro, y así sucesivamente. La práctica en la que las sesiones con direcciones MAC aprendidas mediante un puerto específico se asignan al mismo puerto puede ser útil. En este caso, el tráfico de la sesión pasará a través del mismo puerto en ambas direcciones.

El método estándar para crear canales agregados descrito en la especificación IEEE 802.3ad supone la posibilidad de generar un puerto lógico con base en los puertos físicos distribuidos en varios switches. Para asegurar que a los switches se les informa automáticamente de que algún puerto físico pertenece a un puerto lógico específico, esta especificación sugiere un protocolo de servicio especial: el **protocolo de agregación de control de enlace (LCAP)**. Así, es posible organizar las configuraciones de enlaces agregados que mejoren la tolerancia a las fallas de la red no sólo en las secciones entre dos switches, sino también en topologías más complicadas (figura 16.6).

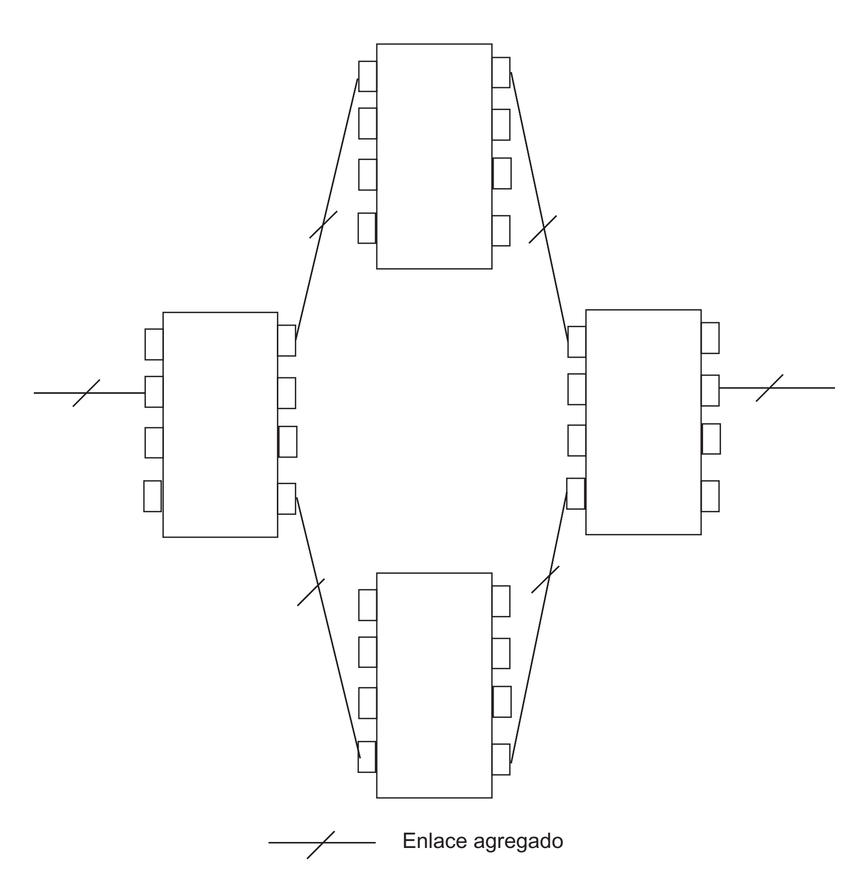


FIGURA 16.6 Agregación de enlace distribuida.

Cuando falla uno de los enlaces agregados dentro de un troncal, todos los paquetes de las sesiones asignados a su puerto correspondiente se dirigirán a uno de los puertos restantes. Por lo regular, un procedimiento de esta clase para restaurar la conectividad se lleva de unos cuantos milisegundos hasta decenas de ellos. Esto ocurre porque en muchas implementaciones troncales, las direcciones MAC mapeadas hacia el enlace físico con fallas se encuentran marcadas de modo convincente como olvidadas. Esta vez, sólo se tienen en cuenta los puertos disponibles. Como los tiempos de descanso en los protocolos de la capa de sesión LAN raras veces son extensos, el tiempo requerido para restablecer la conexión perdida no es demasiado largo.

16.4 LAN VIRTUALES

PALABRAS CLAVE: LAN virtual (VLAN), filtro definido por el usuario, dominio de difusión, concentrador de segmentos múltiples, switch de capa 3, IEEE 802.1Q, IEEE 802.1p, agrupación de puerto, agrupación de direcciones MAC, identificador de formato canónico (CFI, Canonical Format Identifier), identificador de protocolo de etiqueta (TPID, Tag Protocol IDentifier) e información de control de etiqueta (TCI, Tag Control Information).

La capacidad para controlar la transmisión de tramas entre segmentos de red es una propiedad importante de los switches del LAN. Por varias razones, como respetar los derechos de acceso e imponer una política de seguridad, no siempre es necesario transmitir una trama hacia la dirección de destino especificada.

Como se muestra en el capítulo 15, dicha tarea puede llevarse a cabo mediante *filtros definidos por el usuario*. Sin embargo, un filtro de este tipo puede evitar la transmisión de la trama hacia direcciones de destino específicas solamente. Por el contrario, el tráfico de difusión se transmitirá hacia todos los segmentos de la red. Esto lo requiere el algoritmo de puente implementado en los switches. Por lo tanto, las redes creadas con base en puentes y switches a veces se denominan *planas* debido a la ausencia de barreras para propagar el tráfico de difusión.

La tecnología VLAN permite a los administradores superar esta limitación.

La **LAN virtual (VLAN)** es un grupo de nodos de red cuyo tráfico, incluidas las difusiones, está aislado de otros nodos de la red.

Lo anterior significa que es imposible transmitir tramas con base en direcciones de la capa de enlace de datos entre diferentes redes virtuales, sin importar qué clase de dirección se especifique: única, multidirigida o de difusión. Al mismo tiempo, las tramas dentro de una VLAN se transmiten de acuerdo con la tecnología de conmutación (por ejemplo, solamente hacia el puerto relacionado con la dirección de destino de la trama).

Las VLAN se podrán *traslapar* si una o más computadoras participan en más de una VLAN. En el ejemplo ilustrado en la figura 16.7, el servidor de correo electrónico (e-mail) participa en las VLAN 3 y 4. Esto significa que sus tramas se transmiten por switches a todas las computadoras que participan en esas redes. Si una computadora participa sólo en VLAN 3, sus tramas no alcanzarán la red 4. Sin embargo, será capaz de comunicarse con computadoras de la red 4 a través de un servidor de correo común. Un método así no asegura protección completa de las VLAN desde otra porque, por ejemplo, una tormenta de difusión originada en el servidor de correo inundará las redes 3 y 4.

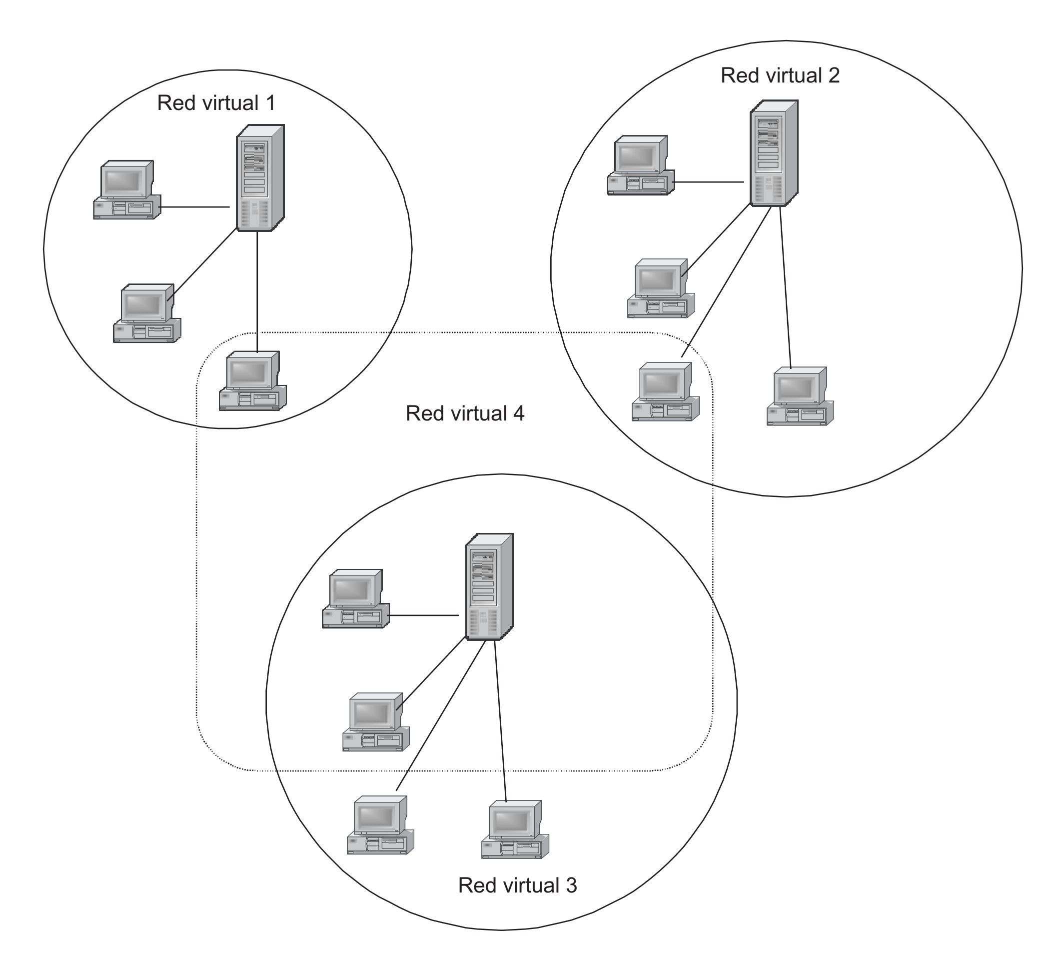


FIGURA 16.7 VLAN.

De este modo, una red virtual conforma un *dominio de difusión,* cuyo nombre es elegido por analogía con un dominio de colisión creado por repetidores Ethernet.

16.4.1 Objetivo de la VLAN

El objetivo principal de la tecnología VLAN consiste en crear redes aisladas, que deben estar conectadas por enrutadores en los que se ponga en marcha algún protocolo de capa de red, como IP. Tal estructura de red genera barreras mucho más confiables, con lo cual se evita la propagación del tráfico indeseable desde una red a otra. En la actualidad se acepta comúnmente que toda red a gran escala debe incluir enrutadores; de otro modo, los flujos de tramas erróneas, como difusiones para las cuales son transparentes los switches, inundarían de manera periódica la red completa e interrumpirían su operación.

> La tecnología VLAN proporciona una base flexible para construir una red a gran escala conectada mediante enrutadores, pues los switches permiten a los administradores producir segmentos aislados por medio de configuración lógica sin utilizar conmutación física.

Antes de que existiera la tecnología VLAN, se creaban redes separadas con segmentos aislados físicamente de cable coaxial, o con segmentos no conectados a otro construido sobre los repetidores y puentes. Más tarde, esas redes aisladas se conectaban a enrutadores en una interconexión de redes completa (figura 16.8).

Al utilizar este enfoque, la introducción de cualquier cambio en estructura del segmento, como mover al usuario a otra red o dividir amplios segmentos, implica la conmutación física de los conectores en los paneles frontales de los repetidores o en los paneles cruzados. Para redes a gran escala, este enfoque no es conveniente, porque implica una enorme cantidad de operaciones manuales y se caracteriza por una alta probabilidad de errores.

Dicho problema se resolvió de manera parcial mediante los concentradores de segmentos múltiples (considerados en el capítulo 14), los cuales eliminaron la necesidad de la conmutación física de los nodos de la red. Esto permitió programar la estructura del segmento compartido sin una reconexión física.

Sin embargo, la solución al problema de cambiar la estructura del segmento con el uso de concentradores fue en realidad sólo parcial, porque implica limitaciones significativas sobre la estructura de la red. Por lo tanto, no es realista esperar que se pudiese asignar un segmento por separado a cada nodo mediante un concentrador así (en contraste con los switches, que son capaces de hacerlo de esa manera). Además, cuando se tiene un enfoque de esta clase, el trabajo completo de transmisión de datos entre los segmentos se delega a los enrutadores, mientras que los switches, con su alto rendimiento, permanecen "sin trabajo". En consecuencia, las redes construidas con base en repetidores con conmutación de configuración se fundamentan en el medio compartido entre muchos nodos y, desde luego, tienen un rendimiento significativamente inferior que las redes construidas con apoyo en switches.

Para conectar VLAN en una interconexión de redes, es necesario utilizar las herramientas de la capa de red. Las funciones de la capa de red pueden realizarse en un enrutador separado o funcionar como parte del software del switch. Nótese que el switch en este caso

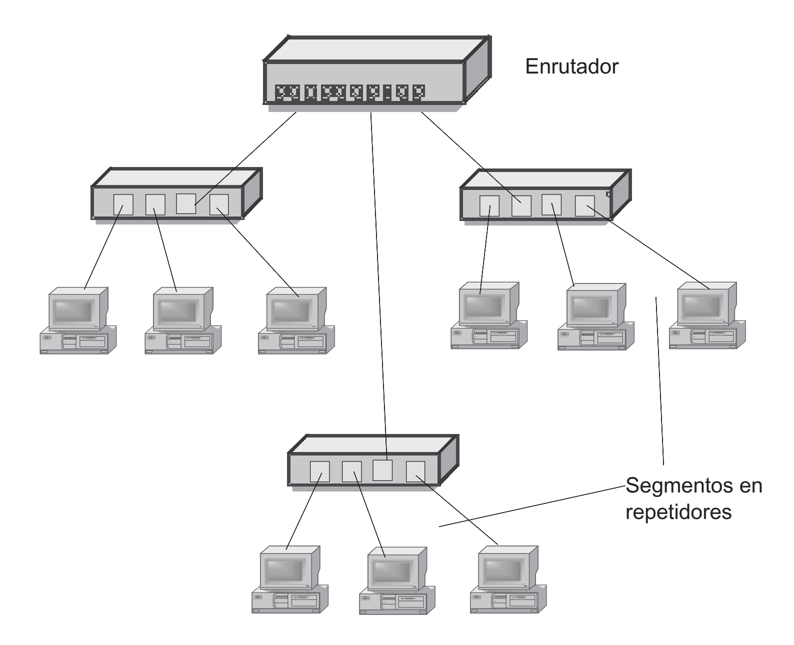


FIGURA 16.8 Interconexión de redes formada por varias redes construidas con base en repetidores.

se convierte en un dispositivo combinado: un **switch de capa 3**. Los switches de este tipo se estudiarán en el capítulo 20.

La tecnología de construcción de VLAN basada en switches y su funcionamiento no se estandarizó durante mucho tiempo, aunque se puso en práctica en una amplia gama de switches de fabricantes distintos. Esta situación cambió en 1998 después de que se adoptó el estándar IEEE 802.1Q, el cual define las reglas básicas de la construcción de VLAN independientes de los protocolos de capa de enlace de datos soportados por un switch.

16.4.2 Creación de VLAN basadas en un switch

Cuando se crean las VLAN basadas en un switch, suele implementarse el mecanismo de una *agrupación de puertos* del switch (figura 16.9). En este caso, cada puerto se asigna a una VLAN específica. La trama que llega desde el puerto perteneciente a otra VLAN (por ejemplo, VLAN 1) nunca se transmite al puerto que no forma parte de esta red virtual. El puerto puede asignarse a varias VLAN, pero esto es raro en la práctica, pues elimina el efecto del aislamiento completo de las redes.

NOTA *Si un segmento creado con base en un repetidor se conecta a uno de los puertos de un switch, no tendrá sentido incluir los nodos de un segmento de esta clase en VLAN diferentes; el tráfico de estos nodos será común en cualquier caso.*

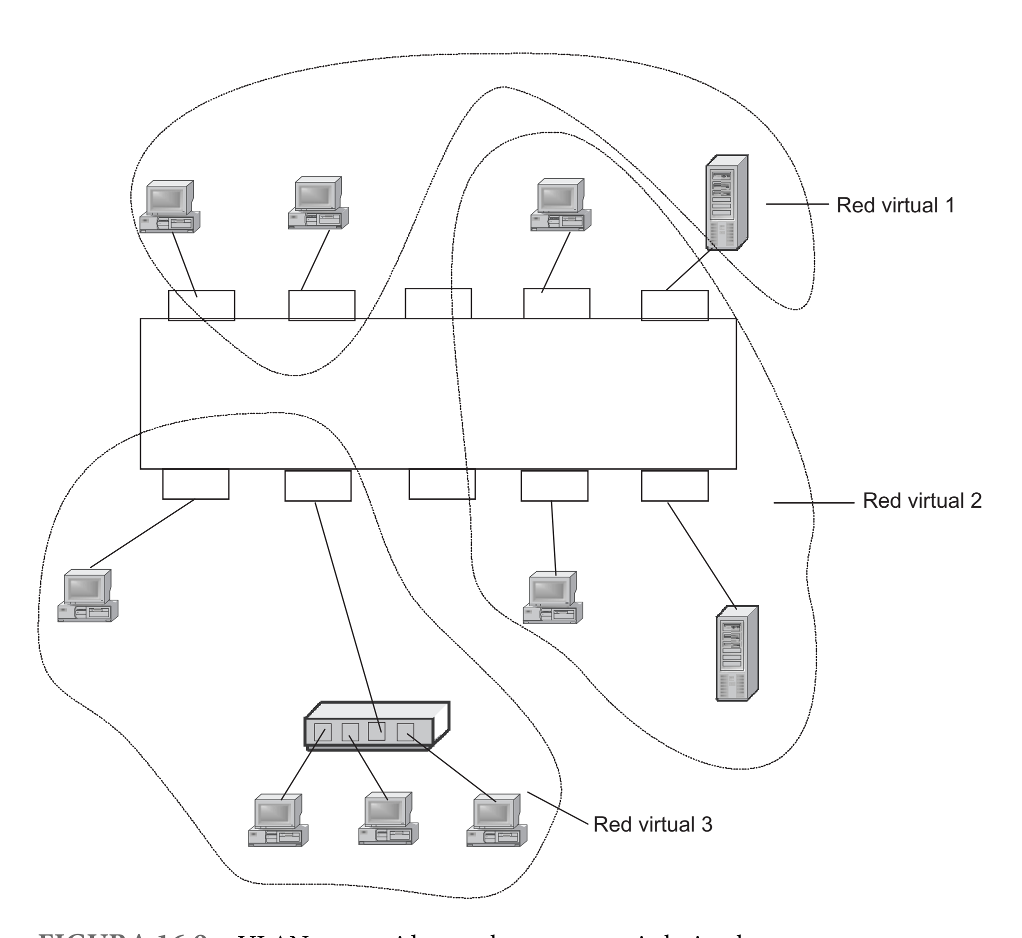


FIGURA 16.9 VLAN construidas con base en un switch simple.

La creación de redes virtuales con apoyo en la agrupación de puertos no requiere gran cantidad de trabajo manual del administrador; es suficiente asignar cada puerto a una de las VLAN nombradas de antemano. Por lo regular, esta operación se lleva a cabo mediante un programa especial suministrado con el switch.

El segundo método para crear VLAN está basado en la *agrupación de direcciones MAC*. Cada dirección MAC aprendida por el switch se asigna a una VLAN específica. Cuando la red consta de varios nodos, este método requiere que el administrador realice múltiples operaciones manuales. Sin embargo, este método da más flexibilidad cuando se construyen VLAN basadas en varios switches que el método de agrupación de puertos.

16.4.3 Creación de VLAN basadas en varios switches

La figura 16.10 ilustra el problema que surge cuando se construyen VLAN con base en varios switches que soportan la técnica de la **agrupación de puertos**.

Si los nodos de algunas VLAN abarcan varios switches, deberá asignarse un par especial de puertos a los switches para interconectar éstos a cada VLAN. De otro modo, cuando los switches se conectan mediante un simple par de puertos, la información de una trama perteneciente a una VLAN específica se perderá cuando se transmita una trama de switch a switch. De esta manera, para conectarse, los switches con agrupación de puertos requieren que el número de los puertos corresponda al número de VLAN soportadas. Los puertos y los cables se utilizan con mucho desperdicio cuando se pone en práctica este método. Además de esto, cuando se conectan VLAN por medio de un enrutador, se asigna un cable por separado y un puerto de enrutador por separado para cada VLAN, lo cual también produce un gasto considerable.

La *agrupación de direcciones MAC* en una VLAN para cada switch elimina la necesidad de conectarlos mediante puertos múltiples, pues en este caso la dirección MAC representa una clasificación de VLAN. Sin embargo, este método requiere numerosas operaciones manuales relacionadas para mapear direcciones MAC a VLAN en cada uno de los switches de la red.

Los dos enfoques descritos aquí se basan sólo en la adición de información auxiliar para las tablas de dirección del switch, pero impiden insertar directamente la trama de información que especifique que una trama pertenece a una VLAN en particular. Los enfoques restantes utilizan campos auxiliares de la trama con el fin de almacenar información en la VLAN de la trama para enviarla de un switch a otro. En este caso, no hay necesidad de otorgarle

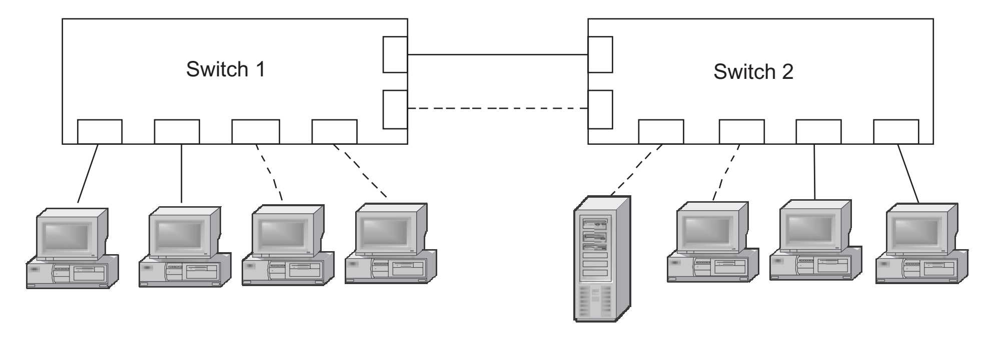


FIGURA 16.10 Construcción de VLAN basadas en varios switches con agrupación de puertos.

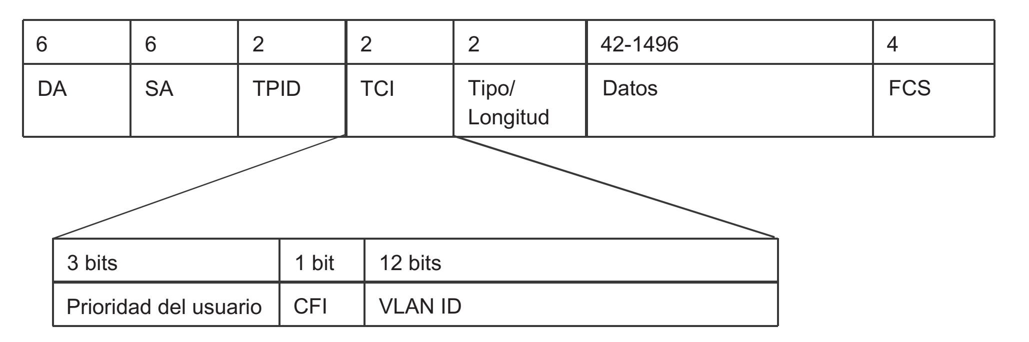


FIGURA 16.11 Estructura de la trama Ethernet clasificada.

información acerca de las direcciones MAC mapeadas a VLAN específicas en cada uno de los switches de la red.

Un campo auxiliar que contenga la marca de una VLAN específica se utiliza solamente cuando la trama se pasa de un switch hacia otro. Cuando se transmite la trama hacia el nodo terminal por lo regular se elimina. En este caso, el protocolo de interacción "switch-switch" se modifica y el hardware y el software de los nodos terminales permanecen igual. Antes de adoptar el estándar IEEE 802.1Q había muchos protocolos propietarios de este tipo. No obstante, estos protocolos tienen una desventaja en común: el equipo de fabricantes diferentes no es compatible cuando se construyen VLAN.

Para almacenar el número de una red virtual, el estándar **IEEE 802.1Q** (también conocido como *protocolo de etiqueta*, debido a que agrega la clasificación al encabezado) proporciona un encabezado adicional de cuatro bytes (figura 16.11). Los primeros dos bytes forman el **identificador del protocolo de etiqueta (TPID**, por sus siglas para **Tag Protocol IDentifier)** y siempre llevan el valor hexadecimal 0x8100, gracias al cual el equipo de redes debe reconocer que esta trama es la trama Ethernet etiquetada. Los siguientes bytes se conocen como **información de control de la etiqueta (TCI**, por sus siglas para **Tag Control Information)** y el protocolo **802.1Q** los comparte con el protocolo **802.1p**, el cual se estudiará en la sección 16.5 ("Calidad del servicio en LAN"). En este campo se utilizan 12 bits para almacenar el número de la VLAN (el campo ID de VLAN o VLAN ID) y se asignan 3 bits para almacenar la prioridad de la trama, como se definió en el estándar 802.1p (el campo de prioridad del usuario, "User Priority"). Para brindar la posibilidad de distinguir las tramas Ethernet de las tramas Token Ring se incluyó un bit, conocido como **identificador de formato canónico (CFI**, por sus siglas para **Canonical Format Identifier)**. En las tramas Ethernet, este bit debe establecerse a 0. El campo VLAN ID de 12 bits permite crear hasta 4 096 redes virtuales. Como el campo de datos de la trama Ethernet disminuye en dos bytes cuando se agrega el encabezado 802.1Q/p, su tamaño máximo también disminuye. Por ejemplo, para la trama Ethernet II, este tamaño es igual a 42-1 496 bytes en contraste con los valores estándar de 46-1 500 bytes.

La adopción del estándar 802.1Q permitió a los fabricantes de equipos superar las diferencias en las implementaciones de VLAN propietarias y obtener la compatibilidad cuando se construyen las VLAN. Las técnicas de VLAN están soportadas por los fabricantes de switches y por los fabricantes de adaptadores de red. En este último caso, el adaptador puede generar y recibir tramas Ethernet clasificadas que contengan el campo VLAN TAG. Si el adaptador de la red genera tramas etiquetadas, las mapea a una VLAN específica. Por lo tanto, el switch debe procesar tales tramas de la manera apropiada (por ejemplo, decidir si

tiene o no que transmitirlas a un puerto de salida específico), lo cual depende del mapeo del puerto a cierta VLAN. El controlador del adaptador de red obtiene el número de su VLAN o sus VLAN de los datos de configuración introducidos manualmente por el administrador de la red; de manera alternativa, podrá recibir esta información de alguna aplicación que se ejecute en el nodo específico. Una aplicación así también puede ejecutarse en uno de los servidores de red centralizados y controlar la estructura completa de la red.

La existencia de VLAN en la red influye en la selección de la topología de árbol de expansión activa. Considérese el ejemplo mostrado en la figura 16.12.

Se tienen dos VLAN en esta red: VLAN1 y VLAN2, las cuales están construidas con base en la técnica de agrupación de puertos. La ilustración muestra las conexiones entre los puertos de la VLAN1 como líneas continuas, mientras que las conexiones entre los puertos de la VLAN2 se exhiben como líneas interrumpidas.

Sin considerar la presencia de las VLAN en esa red cuando se construye la topología STA activa, el resultado será el árbol de expansión mostrado en la figura 16.13 (el switch 1 se eligió como el switch raíz). Esta topología no es eficaz para VLAN2 pues, por ejemplo, la trayectoria desde la computadora W1 hasta el servidor S3 pasa a través de cuatro switches de tránsito. En comparación, la trayectoria desde las computadoras de la VLAN1 hacia el servidor S1 pasa a través de dos switches de tránsito. Si se elige el switch 2 como el switch de tránsito, esa topología será ineficaz para VLAN1.

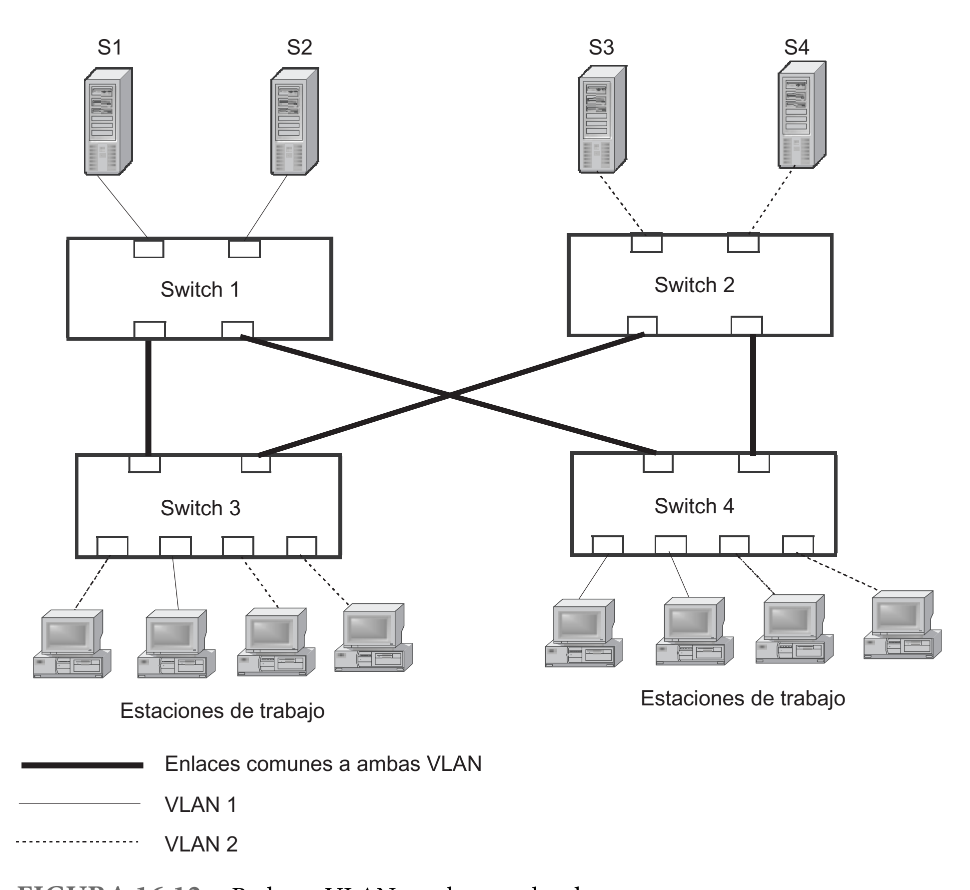


FIGURA 16.12 Red con VLAN y enlaces redundantes.

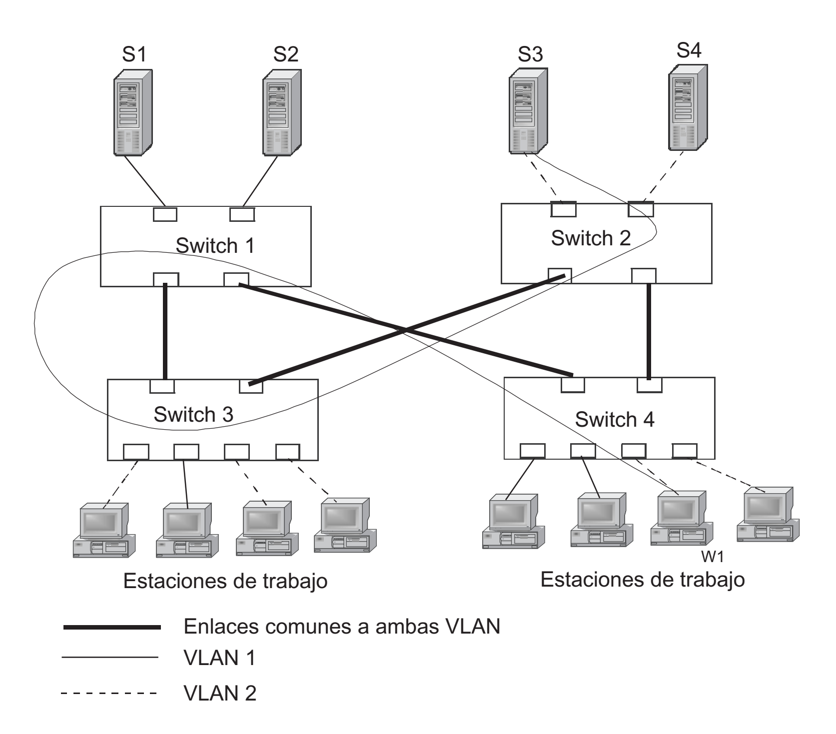


FIGURA 16.13 Árboles extendidos sin tener en cuenta las VLAN.

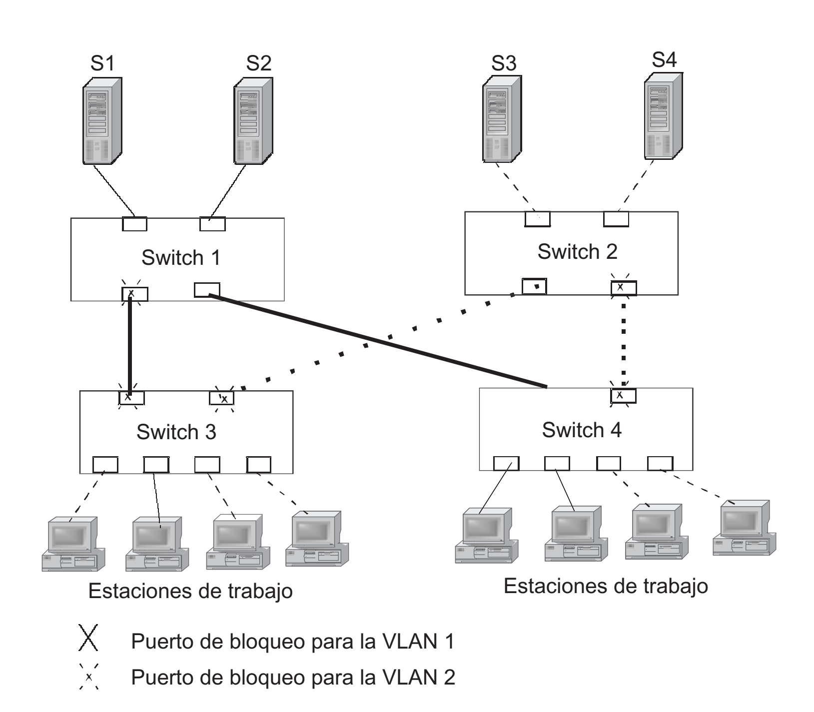


FIGURA 16.14 Árboles extendidos en los que se tienen en cuenta las VLAN.

Otra solución consiste en construir la topología activa por separado para cada VLAN. En el ejemplo considerado, un enfoque de ese tipo produciría dos árboles, con el switch 1 como raíz para la VLAN1 y el switch 2 como raíz para la VLAN2 (figura 16.14).

16.5 CALIDAD DEL SERVICIO EN LAN

PALABRAS CLAVE: 802.1Q/p, clasificación de tráfico, clasificación según el tráfico, ocho clases de tráfico de LAN, tráfico en tiempo no real, tráfico sensible al retardo, administración de las colas y mecanismo de vigilancia.

Los switches de LAN soportan prácticamente todos los mecanismos de QoS descritos en el capítulo 7. Esta afirmación es verdadera para switches de LAN como una clase de dispositivos de comunicación. Por otra parte, cada modelo de switch puede soportar sólo cierto conjunto de mecanismos QoS o no proporcionar soporte para tales mecanismos. Como regla, los switches de grupos de trabajo no soportan QoS, pero para switches troncales este soporte es una obligación.

Clasificación de tráfico. Los switches de LAN son dispositivos de capa 2 que únicamente analizan los encabezados de la capa de enlace de datos. Por lo tanto, los switches suelen clasificar el tráfico con direcciones MAC de origen y destino y el número del puerto al que ha llegado la trama. También es posible emplear para clasificación cualquier subcampo arbitrario dentro del campo de datos, especificado por el desplazamiento del byte. Estos métodos no son muy convenientes para el administrador que necesita, por ejemplo, separar el tráfico de voz del tráfico de transferencia de archivo. En consecuencia, algunos modelos de switches realizan la clasificación con base en los atributos contenidos en los encabezados de protocolos de capa superior sin soportarlos por completo (por ejemplo, sin utilizar IP para direccionamiento de paquetes). Es decir, tal clasificación puede llevarse a cabo según las direcciones IP y atributos de aplicación contenidos en los encabezados de los paquetes.

Etiquetado del tráfico. Éste realiza su clasificación sólo en el margen de la red y usa los resultados de la clasificación en todos los dispositivos de tránsito de la red. La trama Ethernet 802.3 no contiene ningún campo que pudiera almacenar el resultado de clasificación del tráfico. No obstante, esta desventaja es corregida por la especificación 802.1p, que emplea 3 bits del encabezado auxiliar considerado 802.1Q/p para almacenar la prioridad de la trama.

Los tres bits se usan para almacenar una de las ocho clases posibles de tráfico. El estándar 802.1D-1998, que incluye la especificación 802.1p, interpreta dicho campo de esta manera. El apéndice H del estándar 802.1D-1998 da recomendaciones acerca de la división de todo el tráfico de la LAN en las ocho clases enumeradas en la tabla 16.1.

El fondo (BK, por Background) es el tráfico menos sensible a retardos, como el de respaldo, pero la fuente de este tráfico puede transmitir grandes volúmenes de datos; por lo tanto, tiene sentido asignarlo a una clase por separado. Ello asegura que este tráfico no reduzca el procesamiento de otros tipos de tráfico.

Las clases de mejor esfuerzo (BE, Best Effort), esfuerzo excelente (EE, Excellent Effort) y carga controlada (CL, Controlled Load) no son clases en tiempo real, lo cual significa que no imponen requerimientos rigurosos sobre los límites de retardo. No obstante, para estas clases, es deseable asegurar algún nivel mínimo de ancho de banda. Es conveniente atender estas clases por medio del mecanismo de colas ponderadas.

Las clases de video (VI), voz (VO) y control de red (NC, Network Control) son sensibles al retardo. Los valores recomendados de umbrales de retardo se proporcionan en la tabla 16.1. Es conveniente atender a estas clases mediante el mecanismo de prioridad de las colas. La clase de control de red tiene la prioridad más alta, pues todas las características de la red dependen tanto de la toma de decisiones oportuna como de la entrega de la información a los dispositivos de la red.

TABLA 16.1 Clases de tráfico LAN

Prioridad al usuario	Acrónimo	Tipo de tráfico
1	BK	Fondo
2	–	Espacio
0 (Default)	BE	Mejor esfuerzo
3	EE	Esfuerzo excelente
4	CL	Carga controlada
5	VI	“Video”, < 100 ms latencia y “jitter”
6	VO	“Voz”, < 100 ms latencia y “jitter”
7	NC	Control de red

TABLA 16.2 Clases de tráfico y número de colas

<table>
<tr><th>Número de colas</th><th colspan="8">Definición del tipo de tráfico</th></tr>
<tr><td>1</td><td colspan="8">BE</td></tr>
<tr><td>2</td><td colspan="4">BE</td><td colspan="4">VO</td></tr>
<tr><td>3</td><td colspan="4">BE</td><td colspan="2">CL</td><td colspan="2">VO</td></tr>
<tr><td>4</td><td colspan="2">BK</td><td colspan="2">BE</td><td colspan="2">CL</td><td colspan="2">VO</td></tr>
<tr><td>5</td><td colspan="2">BK</td><td colspan="2">BE</td><td>CL</td><td>VI</td><td colspan="2">VO</td></tr>
<tr><td>6</td><td colspan="2">BK</td><td>BE</td><td>EE</td><td>CL</td><td>VI</td><td colspan="2">VO</td></tr>
<tr><td>7</td><td colspan="2">BK</td><td>BE</td><td>EE</td><td>CL</td><td>VI</td><td>VO</td><td>NC</td></tr>
<tr><td>8</td><td>BK</td><td>–</td><td>BE</td><td>EE</td><td>CL</td><td>VI</td><td>VO</td><td>NC</td></tr>
</table>

Administración de las colas. El switch que soporta QoS utiliza varias colas para procesamiento diferenciado de clases de tráfico. Las colas pueden ser atendidas de acuerdo con algoritmos de prioridad de cola o ponderación de cola o con base en su combinación.

Por lo regular, el switch soporta un número máximo de colas, que puede ser más pequeño que el número requerido de clases de tráfico. En esta situación, varias clases serán atendidas por la misma cola, lo cual significa que se mezclarán en la misma clase. El estándar 802.1D-1998 da las siguientes recomendaciones en relación con las clases de tráfico que deben implementarse en la red según un número limitado de colas del switch (tabla 16.2).

Cuando sólo está disponible una cola, únicamente puede existir en la red una clase de tráfico: BE. QoS no puede mejorarse por administración de colas, aunque permanecen disponibles capacidades tales como retroalimentación y reservación de ancho de banda.

Dos colas permiten que el tráfico se divida en dos clases: BE y VO. En tales condiciones, todo el tráfico sensible al retardo debería clasificarse como VO, no sólo para administración de tráfico de voz, sino también de video y de red.

Mientras mayor es el número de colas más fácil es la atención de tráfico diferenciado y el número de clases se incrementan hasta el valor recomendado de ocho.

El método mencionado es solamente una sugerencia y los administradores de red son libres de clasificar el tráfico de acuerdo con sus necesidades. Además, también es posible atender flujos de tráfico individual. Sin embargo, en este caso, todo switch debe separar los flujos individuales de manera independiente desde el tráfico agregado, pues la trama Ethernet no tiene un campo dedicado para transportar una clasificación de flujo a través de la red.

Un número de VLAN también puede utilizarse como atributo de la clase de tráfico, el cual puede combinarse con los valores del campo de prioridad de la trama, campo que permitiría al administrador producir un gran número de clases de tráfico.

Reservación y vigilancia. Los switches LAN soportan los métodos de reservación del ancho de banda para clases de tráfico o flujos individuales. Por lo regular, el switch facilita al administrador asignar a la clase o flujo alguna velocidad de información mínima, garantizada para los periodos de congestión, y la máxima velocidad de información, controlada por los mecanismos de vigilancia.

Para switches de LAN, no hay un protocolo de reservación de recursos estándar. Por lo tanto, para llevar a cabo tales reservaciones, el administrador de la red tiene que configurar individualmente cada switch de la red.

16.6 LIMITACIONES DE PUENTES Y SWITCHES

PALABRAS CLAVE: VLAN, repetidor, puente, switch, libre de ciclos o loops, filtrado de tráfico, direccionamiento, red heterogénea, rendimiento y confiabilidad.

El uso de los switches permite a un administrador superar las limitaciones típicas para las redes basadas en un medio compartido. Las redes conmutadas pueden abarcar territorios significativos y se convierten sutilmente en MAN. También pueden abarcar segmentos con diferentes anchos de banda y formar así redes de muy alto rendimiento. Por último, pueden utilizar rutas alternas para mejorar el rendimiento y la confiabilidad.

Sin embargo, la construcción de complicadas redes basadas sólo en repetidores, puentes y switches (por ejemplo, sin utilizar dispositivos de capa de red) tiene limitaciones y desventajas significativas, a saber:

- En primera instancia, la topología de la LAN conmutada todavía tiene limitaciones considerables. El uso de la técnica STA y la agregación de enlaces elimina las limitaciones impuestas por el requerimiento que prescribe que la red debe ser sólo parcialmente *libre de ciclos o loops*. STA no permite que todas las rutas alternas se utilicen para transmitir tráfico del usuario, y la adición de enlaces favorece esto sólo en las secciones de la red entre dos switches vecinos. Tales limitaciones no permiten muchas topologías eficaces, que podrían utilizarse para la transmisión del tráfico.
- En segundo lugar, los segmentos lógicos de la red localizados entre los switches están *débilmente aislados* de otros, lo cual significa que carecen de protección contra las tormentas de difusión. Aunque la mayoría de los switches que ponen en marcha el mecanismo de VLAN dan flexibilidad en la creación de grupos aislados de estaciones de trabajo que no comparten el tráfico, esta solución no se halla libre de desventajas. El mecanismo de VLAN aísla las VLAN individuales de tal manera que los nodos de una VLAN no pueden comunicarse con los de otra VLAN.

- En tercer lugar, el *problema del filtrado del tráfico* según los valores de los datos contenidos en el paquete no tiene solución simple en redes creadas con base en puentes y switches. En tales redes, esta tarea podrá realizarse si se ponen en práctica filtros definidos por el usuario. Para crear estos filtros, un administrador tiene que tratar con representaciones binarias del contenido del paquete.
- En cuarto lugar, la implementación del subsistema de transporte sólo con herramientas de la capa de enlace de datos y física soportada por los switches produce un sistema de *direccionamiento plano insuficientemente flexible*: una dirección MAC con codificación dura en el adaptador de red se utiliza como la dirección de destino.
- Por último, los switches tienen *capacidades limitadas de traducción de protocolo* cuando se crean redes heterogéneas. Por ejemplo, los switches no pueden traducir protocolos WAN a protocolos LAN debido a las diferencias en los sistemas de direccionamiento de estas redes y los distintos valores del tamaño máximo del campo de datos.

La presencia de serias limitaciones en los protocolos de la capa de enlace de datos muestra que la construcción de redes grandes y heterogéneas con base en las herramientas de la capa de enlace de datos es bastante problemática. La solución natural para estos casos consiste en usar las herramientas de la capa superior de red.

16.7 ESTUDIO DE CASO

En el capítulo 12 se consideró la estructura de la LAN construida con base en repetidores Ethernet de 10 Mbps para necesidades internas de la planta de ingeniería de Transmash. Ese ejemplo corresponde a la situación típica a inicios de la década de 1990, cuando un solo medio compartido de 10 Mbps satisfacía por completo las necesidades de la empresa y permitía el intercambio de tráfico entre computadoras de los departamentos de la empresa, que eran pocas. Aquí se tendrá en cuenta una versión actualizada de la LAN de esta planta de ingeniería, que es un ejemplo típico de la mayoría de las más grandes redes empresariales a finales de la década de 1990.

La principal característica de dicha red es que toda la LAN está construida con switches (figura 16.15). La migración a un diseño de red conmutada se debió a los requerimientos crecientes de rendimiento y confiabilidad de la red. En esa época, el procesamiento de datos computacionales llegó a ser de vital importancia para el proceso de producción. En consecuencia, el número de computadoras se había incrementado bruscamente y se introdujeron aplicaciones más novedosas, que facilitaron intercambiar grandes volúmenes de información multimedia.

Los cimientos de la LAN de cualquiera de los cinco edificios ahora están formados por un poderoso switch central basado en un chasis, equipado con puertos Fast Ethernet y Gigabit Ethernet (switches BS1-BS5). El switch del edificio conecta switches de piso, mediante troncales que combinan dos o tres puertos Fast Ethernet. Cada switch de piso se utiliza para conectar el equipo del usuario final de dos tipos: PC y diversos equipos tecnológicos (estas conexiones se muestran con más detalle en el ejemplo de la LAN del edificio 2). Los usuarios de PC trabajan con aplicaciones que forman el sistema de planeación de recursos corporativos (ERP, Enterprise Resource Planning) automatizado y el equipo tecnológico trabaja con aplicaciones que forman el sistema de fabricación asistida por computadora (CAM, Computer-Aided Manufacturing) automatizada.

Los switches centrales de los edificios 2, 3 y 4 constituyen el troncal de la LAN de la empresa y se encuentran conectados mediante dos troncales Gigabit Ethernet de dos puertos,

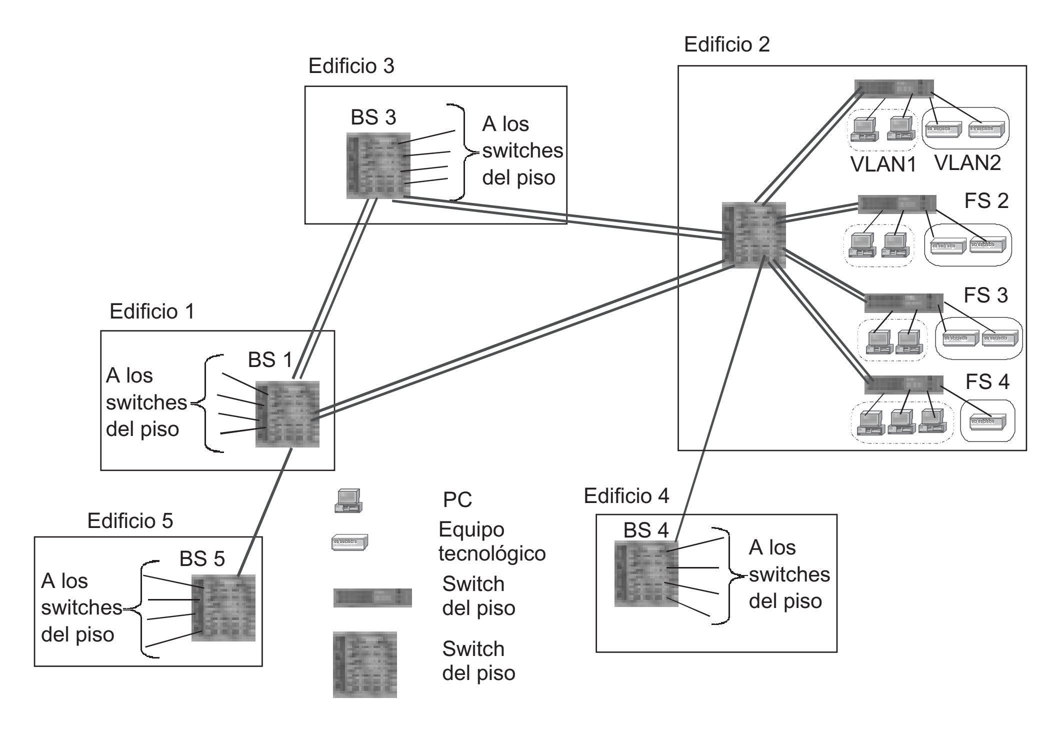


FIGURA 16.15 Red conmutada de la planta de ingeniería Transmash.

lo que asegura una reserva de rendimiento considerable. Los edificios 4 y 5 están conectados al troncal mediante conexiones Gigabit Ethernet normales (sin emplear troncales). Para la conexión de los switches de estos edificios se emplea fibra óptica multimodal, instalada para la LAN basada en repetidores, debido a que su calidad fue satisfactoria para asegurar un funcionamiento estable de los puertos 1000Base-SX.

La red de Transmash transmite dos tipos de tráfico: desde la aplicación ERP y desde aplicaciones CAM. Estas clases de tráfico difieren en sus requerimientos QoS. Por ejemplo, el tráfico CAM es el tráfico en tiempo real, mientras que el tráfico ERP no lo es. Por consiguiente, están organizadas dos VLAN en la red de Transmash: VLAN1 para el tráfico ERP y VLAN2 para el tráfico CAM. Esto permite aislar de modo confiable cada tipo de tráfico y simplifica de manera adicional el soporte QoS por switches, pues el número de VLAN (en este caso, 2) indica que el tráfico debe procesarse en colas de prioridad.

Debido a que el troncal de la LAN tiene enlaces redundantes, los switches utilizan STA de forma individual para cada VLAN. Para la VLAN1, el enlace entre los switches BS4 y BS2 es el enlace de reserva, mientras que VLAN2 es el enlace entre los switches BS4 y BS3. Se consigue el intercambio de datos entre ERP y CAM debido a que varios servidores son miembros de ambas VLAN.

RESUMEN

- Para soporte automático de enlaces reservados en redes complejas, los switches implementan el algoritmo de árbol de expansión (STA, por sus siglas en inglés). Este algoritmo se describe en el estándar IEEE 802.1D. STA está basado en el intercambio periódico por

tramas especiales entre switches. Al usar estas tramas, los switches encuentran y bloquean ciclos o loops cerrados que puedan existir en la red.

- El protocolo STA encuentra la configuración de árbol de expansión al realizar un procedimiento de tres etapas. En la primera etapa, se determina el switch raíz; en la segunda, se encuentran los puertos raíz y en la tercera, se seleccionan los puertos designados de los segmentos.
- La principal desventaja del protocolo STA 802.1D es el tiempo relativamente largo requerido para establecer una nueva configuración activa: aproximadamente 50 segundos. El más reciente estándar 802.1w corrige esta desventaja.
- La agregación de varios enlaces físicos en un canal lógico es una forma de emplear varias rutas alternas en LAN construidas con base en switches.
- La agregación de enlaces mejora tanto la confiabilidad como el rendimiento de la red.
- Un canal agregado no sólo puede crearse entre dos switches vecinos, sino también estar distribuido entre los puertos de varios switches. Para la notificación automática de que un puerto físico específico pertenece a un puerto agregado, se diseñó un protocolo especial, conocido como *protocolo de agregación de control de enlace.*
- La tecnología de las LAN virtuales (VLAN) permite crear grupos aislados de nodos terminales dentro de una red construida con base en switches. No existe ningún tráfico entre estos grupos aislados, incluyendo el tráfico de difusión.
- La configuración de VLAN por lo regular es llevada a cabo por agrupación de puertos. Para construir una VLAN basada en varios switches, es deseable clasificar las tramas transmitidas con una etiqueta especial, de tal modo que se identifique el número de la red a la que pertenece el remitente de esta trama.
- Un formato estándar de la etiqueta de VLAN está definido en la especificación 802.1Q.
- Los switches de LAN soportan todos los tipos de mecanismos QoS: clasificación y vigilancia de tráfico, colas de prioridad y ponderadas, así como reservación del ancho de banda.

PREGUNTAS DE REPASO

1. ¿Cuál es el objetivo de STA?
2. Proporcione una definición del árbol de expansión.
3. ¿Cuál puerto del switch se denomina *puerto raíz*?
4. El puerto designado es el que se define como sigue:
   a) El puerto que se convierte en puerto raíz a discreción del administrador de la red.
   b) El puerto cuya distancia hacia el switch raíz tiene el valor mínimo para un segmento específico.
   c) El puerto conmutado al estado de bloqueo.
5. ¿Cómo es la distancia entre switches medida en STA?
6. Enumere las tres etapas del proceso de construcción de una topología activa de árbol de expansión.
7. ¿Cómo se selecciona el puerto raíz de varios candidatos para este papel si sus distancias desde el switch raíz son iguales?
8. ¿Es posible para un administrador de red influir en la selección del switch raíz?
9. ¿Cómo deciden los switches qué selección de topología activa se ha llevado a cabo?
10. ¿Qué dispara al switch para buscar una nueva topología activa?

11. ¿Cuál es la principal desventaja de STA?
12. La agregación de enlaces:
    a) Mejora el rendimiento de la red
    b) Mejora la confiabilidad de la red
    c) Asegura ambas propiedades
13. ¿En qué casos es más eficaz emplear agregación de enlaces en vez de reconsiderar la versión más rápida de la tecnología Ethernet?
14. ¿Cómo interactúan STA y la agregación de enlace?
15. ¿Cuáles son las limitaciones de las técnicas de agregación de enlaces?
16. ¿Cuál es la diferencia entre un troncal unidireccional y bidireccional?
17. ¿Qué consideraciones se tienen en cuenta cuando se elige el puerto troncal para transmisión de tramas?
18. ¿Por qué es necesario considerar que las tramas pertenecen a la misma sesión cuando se utiliza agregación de enlaces?
19. ¿Por qué la VLAN puede llamarse *dominio de difusión*?
20. ¿Cómo es posible unir varias VLAN?
21. Enumere los métodos principales de creación de VLAN.
22. ¿Por qué la agrupación de puertos es ineficaz en redes basadas en varios switches?
23. ¿Qué enfoque se elige para resolver el problema de construir VLAN basadas en varios switches en el estándar 802.1Q?
24. ¿Es posible utilizar agrupación de puertos y el estándar 802.1Q en conjunto?
25. ¿Es necesario que STA tome en cuenta la presencia de VLAN dentro de la red?
26. ¿Qué mecanismos de QoS son soportados por los switches de LAN?
27. ¿Cuál es el número de clases de tráfico recomendado por el estándar 802.1D-1998?
28. ¿Qué se debería hacer si los switches de la red soportan un número más pequeño de colas que el número de clases de tráfico?
29. Enumere las limitaciones de las redes construidas con base en switches.

PARTE IV

INTERCONEXIÓN DE REDES TCP/IP

Una vez analizada la mayoría de los materiales presentados en este libro, recuérdese lo que se ha estudiado en las primeras tres partes y considérese lo que se aprenderá en las dos partes restantes. En la parte I se examinaron la mayoría de los problemas descritos en este texto a nivel conceptual. Ésta es probablemente la parte más complicada e importante. Después de todo, la calidad del conocimiento y el nivel de las habilidades profesionales dependen en gran medida de los fundamentos en los cuales aquéllos se basan. Muchas veces se ha aludido a los materiales de la parte I, y se continuará haciéndolo así.

Las partes II y III están dedicadas a tecnologías específicas de transmisión de datos en las capas física y de enlace de datos, respectivamente. Los modelos abstractos de red en la forma de una gráfica o una "nube", en la cual "flotan" las computadoras, se encuentran rara vez en estas partes. Por el contrario, los protocolos específicos, los formatos de trama y el equipo de red aparecieron en primer plano.

¿Qué temas se tratarían en la siguiente parte del libro, la cuarta? De acuerdo con la lógica implicada por el modelo OSI, las partes que consideran las tecnologías de la capa física y la de enlace de datos deben estar seguidas por una que considere las herramientas de la capa de red. Estas herramientas aseguran la posibilidad de que haya una interconexión para un gran número de redes en una interconexión de red más grande. Como IP es un líder indiscutible entre todos los protocolos de capa de red, se tienen en cuenta todos los aspectos de interconexión de redes en el ejemplo de este protocolo. Sin embargo, debido a las estrechas relaciones entre IP y los otros protocolos de la pila TCP/IP, se intentará proporcionar un patrón extenso de su interacción.

Nótese que en capítulos anteriores se mencionaron e incluso explicaron diversos aspectos directamente relacionados con el tema de la interconexión de redes TCP/IP. En el capítulo 2 se consideraron las ideas básicas y los principios del enrutamiento. El concepto de interconexión de redes se analizó en el capítulo 4 con información acerca de la capa de red del modelo OSI. De acuerdo con la definición proporcionada, la red general es una combinación de varias redes y se denomina *interconexión de redes* o *internet* ("*interred*"). Las redes que conforman una interconexión de redes se denominan subredes, redes constituyentes o simplemente redes. Las subredes están interconectadas por medio de los enrutadores, mientras que Los componentes de la Internet pueden ser tanto LAN como WAN. Todos los nodos dentro de cada red constituyente se comunican por medio de alguna tecnología común, como Ethernet, Token Ring, FDDI, Frame Relay o X.25. Sin embargo, ninguna de estas tecnologías es capaz de crear un enlace de información entre dos nodos seleccionados arbitrariamente que pertenezcan a redes diferentes. La organización de la interacción entre dos nodos arbitrarios en una Internet se resuelve mediante los protocolos de la pila TCP/IP. En el capítulo 5 se describió la estructura de Internet, la red más grande construida con base en tecnología TCP/IP. Se recomienda mucho al lector revisar este material.

En la última parte del libro, que incluye algunas tecnologías WAN, reconsiderarán el TCP/IP, las características específicas de IP y de ATM/FR, además de la tecnología de etiqueta de conmutación de protocolo múltiple relacionada estrechamente con IP.

La parte IV comprende los capítulos siguientes:

- Capítulo 17: Direccionamiento en redes TCP/IP.
- Capítulo 18: Protocolo de Internet.
- Capítulo 19: Protocolos principales de la pila TCP/IP.
- Capítulo 20: Características avanzadas de los ruteadores IP.

17

DIRECCIONAMIENTO EN REDES TCP/IP

DESCRIPCIÓN DEL CAPÍTULO

17.1 INTRODUCCIÓN

La tecnología TCP/IP está dirigida a resolver los siguientes problemas de direccionamiento:

- *Coordinar el uso de diferentes tipos de direcciones*. Esto incluye el mapeo de direcciones de diferentes tipos, por ejemplo: traducir una dirección IP de red en una dirección local o mapear un nombre de dominio a una dirección IP específica.
- *Asegurar la unicidad de la dirección*. Según el tipo de dirección que se emplee, es necesario asegurar la unicidad del direccionamiento dentro de los límites de la computadora específica, subred, intrarred, red corporativa extendida o Internet.
- *Configurar las interfases de red y las aplicaciones en la red.*

Cada uno de estos problemas tiene una solución bastante simple para redes con sólo decenas de nodos. Por ejemplo, para mapear un nombre de dominio simbólico a una dirección IP específica, es suficiente soportar en cada anfitrión una tabla de todos los nombres simbólicos utilizados dentro de la red y sus mapeos a las direcciones IP. La asignación manual de direcciones únicas a todas las interfases dentro de una red pequeña tampoco es una tarea difícil. No obstante, en redes a gran escala, estas tareas se convierten en algo tan complicado que requieren principalmente soluciones distintas.

La escalabilidad se convierte en una clave que caracteriza el enfoque para resolver estos problemas.

Los procedimientos proporcionados por TCP/IP para la asignación, mapeo y configuración de direcciones funcionan igualmente bien en redes de varias escalas. En este capítulo, además de las opciones para el direccionamiento de IP, se estudiarán las herramientas escalables más conocidas para asegurar el soporte del direccionamiento en redes TCP/IP: enrutamiento entre dominios sin clases (CIDR, por sus siglas para Classless Interdomain Routing), sistema de nombres de dominio (DNS) y protocolo de configuración de anfitrión dinámico (DHCP).

17.2 TIPOS DE DIRECCIÓN DE LA PILA TCP/IP

PALABRAS CLAVE: direcciones local/hardware, direcciones MAC, direcciones redes/IP, direcciones simbólicas/nombres de dominio, número de red, protocolo de resolución de dirección (ARP, Address Resolution Protocol) y sistema de nombre de dominio (DNS, Domain Name System).

Para identificar las interfases de red se utilizan los siguientes tipos de direcciones en redes TCP/IP:

- Direcciones locales (hardware).
- Direcciones de red (IP).
- Direcciones simbólicas (nombres de dominio).

17.2.1 Direcciones locales

La mayoría de las tecnologías LAN, como Ethernet, FDDI y Token Ring, utilizan **direcciones MAC** para identificación de interfases. Existen muchas otras tecnologías (por ejemplo, X.25, ATM y Frame Relay) que usan diferentes sistemas de direccionamiento. Estos sistemas

también permiten identificar las interfases de red dentro de los límites de cada red construida con base en su respectiva tecnología. Como es autónoma, una red así emplea el sistema de direccionamiento exclusivamente para propósitos internos, con lo cual asegura la conectividad de sus nodos. Sin embargo, en cuanto una red específica se conecta a otras redes, la funcionalidad de estas direcciones se extiende. Llegan a convertirse en un elemento obligatorio de la tecnología de interconexión de redes de capa superior, en este caso la tecnología TCP/IP. El papel desempeñado por estas direcciones en TCP/IP no depende de la tecnología específica de interconexión de redes utilizada en la red constituyente. Por lo tanto, estas direcciones tienen el nombre común de **direcciones locales (de hardware)**.

ATENCIÓN *Las definiciones empleadas aquí (local y hardware) pueden interpretarse de manera ambigua. El término local en el contexto de TCP/IP significa que la dirección se encuentra vigente dentro de la red constituyente, pero no dentro de los límites de la interred completa. Éste es el sentido en el que se deben interpretar los términos siguientes: tecnología local (la tecnología con base en la cual se construye la red constituyente) y dirección local (la dirección utilizada por la tecnología local para el direccionamiento de nodos dentro de la red constituyente). Recuérdese que la red constituyente (local) puede construirse con apoyo en una tecnología WAN (X.25, Frame Relay, etc.) o en una LAN (Internet, FDDI, etc.). La palabra local también se utiliza en una LAN (Local Area Network, red de área local). Sin embargo, tiene ahí un significado diferente y caracteriza los aspectos específicos de la tecnología que limita la red a pequeñas distancias.*

También puede haber dificultades con la interpretación del término hardware en el contexto de la interconexión de redes. En este caso, el término destaca que los diseñadores de la pila TCP/IP interpretan una red constituyente como una herramienta de hardware auxiliar, cuyo único objetivo es entregar paquetes IP mediante el uso de la red constituyente hacia el enrutador más cercano. La tecnología de red subyacente puede ser complicada, pero esto es de poca importancia porque se descartan estos detalles de la tecnología TCP/IP.

Por ejemplo, considérese una situación en la que una interred TCP/IP incluye una red constituyente IPX/SPX. Esta última debe dividirse en subredes. De manera similar a la red IP, también identifica sus nodos con direcciones de hardware y direcciones de red IPX. No obstante, TCP/IP ignora la jerarquía de capa múltiple de la red IPX/SPX y la considera, como la red Ethernet, una red constituyente normal. En consecuencia, la tecnología TCP/IP tiene en cuenta las direcciones de red de la red IPX/SPX como direcciones locales. Asimismo, si la red constituyente está construida sobre la tecnología X.25, las direcciones X.25 las analizará la tecnología IP como direcciones locales.

17.2.2 Direcciones de red IP

Para llevar a cabo su tarea de interconectar redes, la tecnología TCP/IP debe tener su propio *sistema de direccionamiento global que no dependa de los métodos de direccionamiento de nodos en las redes constituyentes.* Ese sistema de direccionamiento ha de proporcionar un método universal que identifique de manera única cada interfase de la interred.

Un método natural de formar direcciones de red consiste en identificar de manera única todas las redes constituyentes y numerar los nodos dentro de los límites de cada red. De este modo, una **dirección de red** es un par de números: un **número de red** y un **número de nodo**.

Como un número de nodo, los números siguientes deben utilizarse: la dirección local de ese nodo (un método así se ha adoptado en la pila IPX/SPX) o algún número que identifique de manera única el nodo dentro de la subred, pero que no esté relacionado con la tecnología local.

En el primer caso, la dirección de red depende de las tecnologías locales, lo que limita su área de aplicación. Por ejemplo, las direcciones de red IPX/SPX están dirigidas para usarlas en las interredes que conectan redes que utilizan sólo direcciones MAC o direcciones de un formato semejante. El segundo enfoque es más universal y característico de la pila TCP/IP.

En la tecnología TCP/IP, la dirección de red se denomina **dirección IP**.

ATENCIÓN *Considérese una red IP. El enrutador, por definición, participa en varias redes. Por lo tanto, cada una de sus interfases tiene su propia dirección IP. Cada nodo también puede participar en diversas redes IP, en cuyo caso la computadora debe tener suficientes direcciones IP para el número de enlaces de red. De esta manera, una dirección IP identifica un enlace de red más que una computadora o enrutador específicos.*

Cuando el paquete se envía al receptor a través de la interred, su encabezado debe contener la dirección IP del nodo de destino. Cada enrutador encuentra la dirección IP del siguiente enrutador mediante el número de la red de destino. Antes de enviar el paquete a la siguiente red, el enrutador, basado en la dirección IP del enrutador siguiente, debe determinar su dirección local. Para este propósito, IP utiliza el *protocolo de resolución de dirección* (ARP), como se muestra en la figura 17.1.

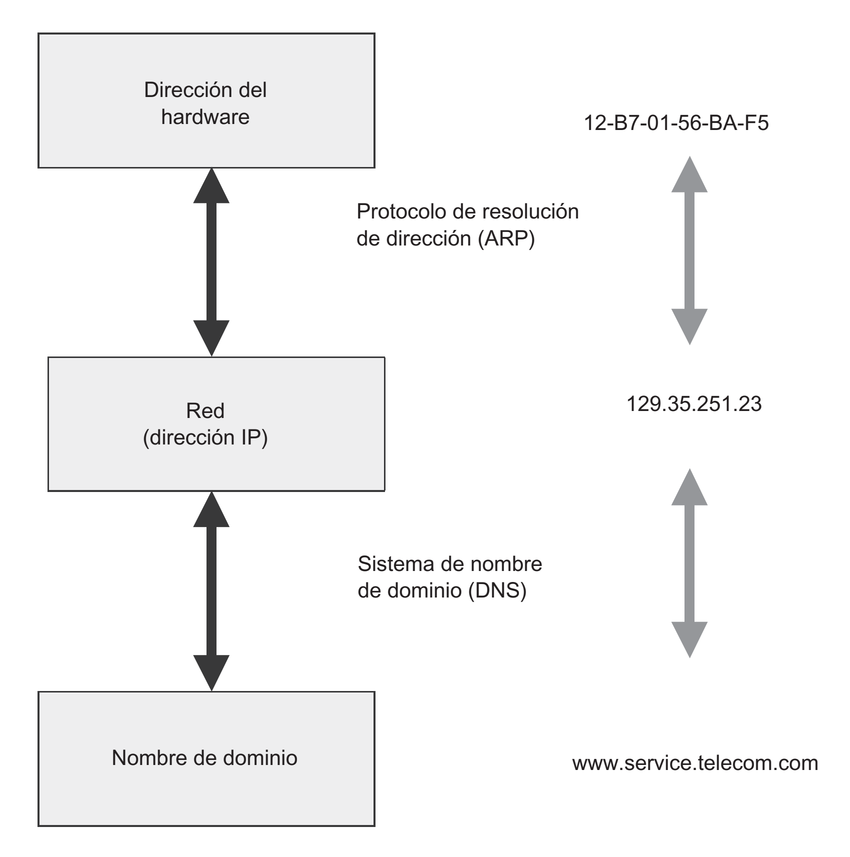


FIGURA 17.1 Protocolo de resolución de dirección (ARP).

17.2.3 Nombres de dominio

El hardware y el software de las redes TCP/IP cuentan con las direcciones IP para la identificación de las computadoras. Por ejemplo, el comando **ftp://192.45.66.17** establecerá la sesión con el servidor ftp requerido, mientras que el comando **http://203.23.106.33** abrirá una página de inicio en el servidor Web corporativo. Sin embargo, la mayoría de los usuarios prefiere tratar con los nombres simbólicos de las computadoras. En consecuencia, las redes TCP/IP deben idear nombres simbólicos para los *host* o anfitriones y un mecanismo para relacionar o "mapear" los nombres simbólicos a las direcciones IP.

Los identificadores simbólicos de las interfases de red dentro de los límites de la interred se construyen de acuerdo con el principio jerárquico. Los componentes del nombre o dominio simbólico completamente calificado en las redes IP están delimitados por puntos decimales y se enumeran en el orden siguiente: en nombre del *host* individual, en nombre del grupo específico del *host* (el nombre de la organización, por ejemplo), el nombre de un grupo más grande (dominio) y así sucesivamente hasta el nombre del dominio de más alto nivel, como el que agrupa organizaciones de acuerdo con su ubicación geográfica: **us** para Estados Unidos (**U**nited **S**tates), **ru** para **Ru**sia y **uk** para Gran Bretaña o Reino Unido (**U**nited **K**ingdom). Un nombre de dominio puede parecerse al que sigue: **server2.janet.ac.uk**.

No hay dependencia funcional entre el nombre del dominio y la dirección IP de un *host*. Por lo tanto, el único método para mapear los nombres simbólicos a direcciones IP usa tablas. Las redes TCP/IP utilizan un servicio especial distribuido, el sistema de nombre de dominio (DNS), el cual establece este mapeo de acuerdo con las tablas de mapeo creadas por administradores de red. Debido a esto, lo nombres de dominio se conocen a menudo como **nombres DNS**.

En general, una interfase de red puede tener de manera simultánea una o más direcciones locales, una o más direcciones de red y uno o más nombres de dominio.

17.3 FORMATO DE DIRECCIÓN IP

PALABRAS CLAVE: formato de dirección IP, máscara, clases de dirección IP, clase A, clase B, clase C, clase D, clase E, unicast, multicast, transmisión, transmisión limitada, dirección definida y anillo.

El encabezado del paquete IP tiene dos campos para almacenar las direcciones IP del emisor y del receptor. Cada campo tiene una longitud fija de 4 bytes (32 bits). La dirección IP es una combinación de dos componentes lógicos: el número de red y el número de host dentro de la red.

La forma más conocida de escribir direcciones IP es la notación con cuatro números, que representa el valor de cada IP en notación decimal y está delimitada mediante puntos. Una dirección IP típica escrita en esta notación punteada tiene el aspecto siguiente:

```
128.10.2.30
```

La misma dirección puede ser representada en el formato binario:

```
10000000 00001010 00000010 00011110
```

También es posible mostrar la dirección IP en el formato hexadecimal:

```
80.0A.02.1D
```

Nótese que el formato de la dirección no proporciona una demarcación especial entre el número de la red y el número de host. Sin embargo, cuando se transmite el paquete a través de la red, a menudo es necesario dividir la dirección en estas dos partes. Por ejemplo, como regla, el enrutamiento se lleva a cabo con base en el número de red. Por consiguiente, cada enrutador, una vez que ha recibido el paquete, debe leer un campo apropiado del encabezado del paquete para encontrar la dirección del host de destino y así localizar el número de red en esta dirección. ¿Cómo pueden determinar los enrutadores qué parte de los 32 bits asignados para almacenar la dirección IP se relaciona con el número de red y qué parte se vincula con el número de host?

Se pueden sugerir varias soluciones para este problema.

- La más simple consiste en utilizar la **frontera fija**. En este caso, todo el campo de 32 bits de la dirección se divide en dos partes por anticipado. Estas partes deben tener longitudes fijas, pero no necesariamente iguales. Una parte debe contener siempre el número de red, mientras que la otra está asignada para almacenar el número de host. Esta solución es muy simple, pero ¿es lo suficientemente buena? No. Como el campo asignado para almacenar el número de host cuenta con una longitud fija, todas las redes tendrán el mismo número máximo de nodos. Por ejemplo, supóngase que usted ha asignado sólo el primer byte para almacenar el número de red. En este caso, todo el espacio de dirección se dividirá en un número relativamente pequeño (2^8) de redes grandes (cada una con hasta 2^{24} hosts). Si usted mueve esta frontera hacia la derecha, tendrá más redes, pero todas ellas serán del mismo tamaño. Obviamente, un enfoque así de rígido no proporciona los medios para diferenciar las necesidades de las organizaciones individuales. Por ello, este método de estructura de direcciones no tiene una aplicación extendida, aunque se utilizó en la etapa inicial de la evolución TCP/IP, como se define en el RFC 760.
- El segundo enfoque (RFC 950 y RFC 1518) se basa en el uso de una **máscara**, que proporciona flexibilidad máxima cuando establece la frontera entre el número de red y el número de host. Cuando se utiliza este enfoque, todo el espacio de dirección puede representarse como un conjunto de redes de diversos tamaños.

> La máscara representa el número empleado con la dirección IP. La representación binaria de la máscara contiene una secuencia de unos binarios en las posiciones de la dirección IP que deben interpretarse como el número de red. La frontera entre la secuencia de unos y la secuencia de ceros en la máscara corresponde a la frontera entre el número de red y el número de host en la dirección IP.

- Finalmente, el tercer enfoque, que fue el más conocido hasta hace poco, usa **clases de dirección IP** como se define en RFC 791. Este método es un compromiso entre los dos enfoques descritos: ante los tamaños de red no son arbitrarios, como cuando se utilizan máscaras, ni son fijos, como cuando se establecían fronteras fijas. Se definen cinco clases de direcciones, tres de las cuales las emplea el direccionamiento de la red, mientras que las dos restantes, como se mostrará más adelante, están reservadas para propósitos especiales.

17.3.1 Clases de direcciones IP

Los valores de varios bits de inicio de la dirección sirven como el criterio con el cual se clasifican las direcciones IP. La tabla 17.1 da una idea general de la estructura de direcciones IP para diferentes clases de dirección.

TABLA 17.1 Clases de direcciones IP

Clase	Primeros bits	Número de red más pequeño	Número de red más grande	Número de nodos
A	0	1.0.0.0 (0 – no usado)	126.0.0.0 (127 – reservado)	2^{24} (3 bytes)
B	10	128.0.0.0	191.255.0.0	2^{16} (2 bytes)
C	110	192.0.0.0	223.255.255.0	2^{8} (1 byte)
D	1110	224.0.0.0	239.255.255.255	Direcciones multicast
E	11110	240.0.0.0	247.255.255.255	Reservado

- La **clase A** incluye las direcciones en las cuales el bit más significativo tiene el valor **0**. En las redes de clase A, 1 byte se asigna para la dirección de red, mientras que los 3 bytes restantes se interpretan como el número de host dentro de la red. Las redes en las cuales todas las direcciones IP tienen un valor de primer byte que abarca desde el 1 (**0**0000001) hasta el 126 (**0**1111110) se conocen como redes de clase A. La red 0 (**0**0000000) no se utiliza y la red número 127 ((**0**1111111) está reservada para propósitos especiales, que se estudiarán con detalle más adelante en este capítulo. Las redes de clase A no son numerosas, pero el número de hosts en tales redes puede llegar a 2^{24} (es decir, 16 777 216).
- La **clase B** incluye todas las direcciones en las cuales los dos bits más significativos se establecen al valor **10**. En la clase B, las direcciones de 2 bytes se han asignado para almacenar el número de red y el número de host. Las redes en las cuales los valores de los primeros 2 bytes de direcciones pertenecen al intervalo desde 128.0 (**10**000000 00000000) hasta 191.255 (**10**111111 11111111) se conocen como redes de clase B. Naturalmente, estas redes son más numerosas que las de clase A, pero sus tamaños son más pequeños. El número máximo de nodos en una red de clase B es de 2^{16} (o sea, 65 536).
- La **clase C** incluye todas las direcciones en las cuales los tres bits más significativos se establecen a **110**. En las redes de clase C, 3 bytes están asignados para el número de red, mientras que 1 byte lo está para el número de host. Las redes en las cuales los 3 bytes más significativos en la dirección IP pertenecen al intervalo desde 192.0.0 (**110**00000 00000000 00000000) hasta 223.255.255 (**110**11111 11111111 11111111) se conocen como redes de clase C, que son las más extendidas, pero el número de hosts en tales redes está limitado a 2^{8} (256).
- Si una dirección IP comienza con la secuencia **1110**, pertenecerá a la **clase D** y es una *dirección de grupo* específica. En contraste con las direcciones de las clases A, B y C, utilizadas para identificar interfases de redes específicas (por ejemplo, direcciones **unicast**), una dirección de grupo se conoce como **dirección multicast**. Las direcciones de grupo identifican a grupos interfases de red, que suelen pertenecer a redes diferentes. La interfase incluida en un grupo, aparte de la dirección IP individual, está asignada a una dirección de grupo. Si una dirección de clase D se especifica como la dirección de destino cuando se envía un paquete, un paquete así deberá entregarse a todos los hosts incluidos en ese grupo.

- Si una dirección IP comienza con la secuencia **11110**, será una dirección de **clase E**. Las direcciones de esta clase están reservadas para usos futuros.

NOTA *Para obtener el número de redes y el número de host aparte de la dirección, es necesario dividir la dirección en dos partes apropiadas y luego complementar cada parte con ceros para llenar 4 bytes. Por ejemplo, supóngase que usted tiene la siguiente dirección de clase B: 129.64.134.5. Los primeros 2 bytes identifican la red y los siguientes 2 bytes especifican el número de host. De este modo, usted tiene un número de red de 129.64.0.0 y número de host de 0.0.134.5.*

17.3.2 Direcciones IP especiales

TCP/IP tiene un límite para la asignación de direcciones IP: los números de red y los números de host *no pueden constar sólo de unos o ceros binarios*. Por lo tanto, el número máximo de hosts proporcionados en la tabla 17.1 para redes de cada clase debe disminuirse a 2. Por ejemplo, en las direcciones de clase C, 8 bits se asignan para almacenar el número de host. Esto permite especificar 256 números: desde el 0 hasta el 255. En realidad, el número máximo de hosts en las redes de clase C no puede exceder de 254, pues los números de host 0 y 255 no están permitidos para su asignación a interfases de red. De acuerdo con las mismas consideraciones, un nodo terminal no puede tener una dirección IP tal como 98.255.255.255, debido a que en esta dirección de clase A, el número de host (0.255.255.255) incluye sólo unos binarios.

Así, algunas direcciones IP colocadas en el encabezado de un paquete IP se interpretan de una manera específica:

- Si la dirección IP consiste por completo en ceros binarios, se conocerá como una **dirección indefinida** y especificará la dirección del host que generó este paquete. En casos especiales, una dirección de este tipo se coloca en el encabezado del paquete IP en el campo de la dirección fuente.
- Si el campo del número de red está llenado completamente con ceros, el host de destino pertenecerá de forma predeterminada a la misma red que el host que envió el paquete. Una dirección así también puede utilizarse sólo como la dirección fuente.
- Si todas las posiciones de la dirección IP están llenas con unos, el paquete con tal dirección de destino deberá enviarse a todos los hosts localizados en la misma red como la fuente de este paquete. Tal tipo de entrega se conoce como **transmisión limitada**. La limitación en este caso significa que el paquete nunca dejará dicha red.
- Si todas las posiciones correspondientes al número de host del host de destino están llenas con unos, el paquete con una dirección así se enviará a **todos** los hosts de la red, cuyo número está especificado en la dirección de destino. Por ejemplo, el paquete que contiene la dirección 192.190.21.255 en el campo de host de destino se enviará a todos los hosts pertenecientes a la red 192.190.21.0. Este tipo de entrega se conoce como **transmisión** (**broadcast**).

ATENCIÓN *IP no introduce el concepto de transmisión en el sentido normalmente utilizado en los protocolos LAN de capa de enlace de datos, donde los datos deben entregarse a todos los hosts sin excepciones. Tanto las transmisiones limitadas de IP como las transmisiones IP tienen restricciones de propagación dentro de las interredes; están limitadas ya sea por las fronteras de la red a la que el host fuente pertenece o por la*

red cuya dirección está especificada en la dirección de destino. Por lo tanto, la división de la red con enrutadores localiza tormentas de transmisión dentro de los límites de una de las subredes simplemente porque no hay método de direccionamiento del paquete a todos los hosts de la interred de manera simultánea.

En las direcciones IP, cuyo primer octeto se ha establecido en 127, esto tiene un significado especial. Esta dirección es de índole de una dirección interna de la computadora o pila del protocolo del enrutador. Se utiliza para programas de prueba y para organizar la operación de los componentes del cliente y servidor de la misma aplicación instalada en la misma computadora. Ambos componentes de la aplicación cliente-servidor se han diseñado con la expectativa de que intercambiarán mensajes mediante el uso de la red. No obstante, cuando se instalan en la misma computadora, ¿cuál dirección IP deberían utilizar para este propósito? Es posible usar la dirección de la interfase de la red del host donde están instalados ambos componentes. Sin embargo, en este caso, inevitablemente se transmitirán paquetes redundantes en la red; por ende, esta solución no es eficaz. Usar la dirección interna 127.0.0.0 es una solución más eficaz y económica. Como el lector recordará, no se permite que las direcciones IP a partir de 127 se asignen a interfases de red. Cuando un programa envía datos a una dirección IP tal como 127.x.x.x, estos datos no se transmitirán en la red. En vez de esto, dichos paquetes se devolverán a las entidades del protocolo de capa superior de la misma computadora como datos apenas recibidos desde la red. La ruta de tales datos realiza un bucle o ciclo; por lo tanto, esta dirección se conoce como **anillo**.

Las direcciones **multicast** pertenecientes a la clase D se han destinado para la distribución económica de programas de audio y video a una gran audiencia sobre la Internet o una red extendida empresarial. Si se coloca una dirección multicast en el campo de dirección de destino del paquete IP, un paquete de esta naturaleza deberá entregarse a varios nodos que forman el grupo con el número especificado en el campo de dirección. El mismo host puede pertenecer a varios grupos. Los miembros de un grupo multicast específico no necesariamente deben pertenecer a la misma red; en general, pueden estar distribuidos sobre diferentes redes ubicadas a cualquier distancia entre sí. Las direcciones multicast no están divididas en números de red y números de host. Los enrutadores procesan tales direcciones de una manera específica.

El objetivo principal de las direcciones multicast consiste en distribuir la información en un arreglo "de uno a muchos". Por el momento, las direcciones multicast se emplean únicamente dentro de pequeños segmentos experimentales dentro de Internet, comparables con islas en el océano. Si Internet llegará o no a ser un competidor serio para las compañías difusoras de radio y televisión dependerá de si estas direcciones multicast llegarán o no a ser populares.

17.3.3 Uso de máscaras en el direccionamiento IP

Al suministrar a cada dirección IP una máscara permite abandonar el concepto de clases de dirección, lo cual hace más flexible el sistema de direccionamiento.

Como recordará el lector, para clases de red estándar, las máscaras de red tienen los valores siguientes:

Clase A	11111111.00000000.00000000.00000000	(255.0.0.0)
Clase B	11111111.11111111.00000000.00000000	(255.255.0.0)
Clase C	11111111.11111111. 11111111.00000000	(255.255.255.0)

La idea principal de este enfoque es utilizar máscaras, en las que el número de unos binarios en la secuencia determinando la frontera del número de red no debe ser necesariamente un múltiplo de ocho (en cuyo caso, las direcciones se dividen en bytes), como con las máscaras de red estándar. Por ejemplo, si usted asocia la dirección 185.23.44.206 con la máscara 255.255.255.0, el número de red se establecerá a 185.23.44.0 en lugar de a 185.23.0.0, como lo definía el sistema de clases.

Considérese otro ejemplo: supongamos que la máscara 255.255.128.0 está especificada para la dirección IP establecida a 129.64.134.5. En formato binario, esto significaría lo siguiente:

Dirección IP	129.64.134.5	10000001.01000000.10000110.00000101
Máscara	255.255.128.0	11111111.11111111.10000000.00000000

Si usted ignora la máscara e interpreta la dirección 129.64.134.5 con base en las clases de dirección, 129.64.0.0 será el número de red, mientras que 0.0.134.5 será el número de host, pues su dirección pertenece a la clase B.

Si usted utiliza la máscara, la secuencia de 17 unos binarios consecutivos en la máscara 255.255.128.0, al "aplicarse" a esta dirección IP, la dividiría en las dos partes siguientes:

		Número de red	**Número de host**
Dirección IP	129.64.134.5	10000001.01000000.1	0000110.00000101
Máscara	255.255.128.0	11111111.11111111.1	0000000.00000000

En notación decimal, el número de red y los números de host completados por medio de ceros a 32 bits serán 129.64.128.0 y 0.0.6.5, respectivamente.

La aplicación de una máscara puede interpretarse como llevar a cabo una operación AND lógica.

Por ejemplo, en este caso, el número de red obtenido de la dirección IP 129.64.134.5 es el resultado de una operación AND lógica con la máscara 255.255.128.0:

(10000001 01000000 10000110 000001011) AND (11111111.11111111.10000000.00000000)

NOTA *Pueden utilizarse otros formatos para máscaras. Por ejemplo, es conveniente interpretar los valores de máscara en código hexadecimal: FF.FF.00.00 es la máscara para las redes de clase B. Otra forma de notación se encuentra con frecuencia: 185.23.44.206/16 significa que la máscara para esta dirección contiene 16 unos, es decir, en esta dirección IP, 16 bits están asignados para el número de red.*

El mecanismo de las máscaras se usa ampliamente en el enrutamiento IP. En el enrutamiento, las máscaras pueden utilizarse para varios propósitos. Por ejemplo, un administrador de red puede emplearlas para dividir una red simple de una clase específica, asignada a la compañía por su proveedor de servicios de Internet (ISP), en varias subredes sin números de red adicionales del ISP. Esta operación se conoce como **subredes (subnetting)**. Con base en dicho mecanismo, los ISP pueden conectar los espacios de dirección de varias redes mediante la introducción de los denominados prefijos para reducir el tamaño de las tablas de enrutamiento y mejorar el rendimiento del enrutamiento de la red. Esta operación se denomina **superredes (supernetting)**, lo cual se estudiará con más detalle posteriormente en este capítulo cuando se describa la tecnología CIDR.

17.4 ORDEN DE ASIGNACIÓN DE DIRECCIÓN IP

PALABRAS CLAVE: direcciones privadas, Corporación de Internet para Asignación de Nombres y Números (ICANN, Internet Corporation for Assigned Names and Numbers), prefijo, colisiones de dirección, espacio de dirección, escasez de direcciones, CIDR y NAT.

De acuerdo con su definición, el método de direccionamiento IP debe asegurar la unicidad de la numeración de red, así como la unicidad de la numeración de host dentro de los límites de cada red. Por consiguiente, los procedimientos de asignación de números tanto para redes como para hosts deben **centralizarse**. La orden recomendada para asignar direcciones IP se describe en RFC 2050.

17.4.1 Asignación de dirección en una red autónoma

Cuando se llega a una red que es parte de Internet, la unicidad de la numeración puede asegurarse sólo con los esfuerzos coordinados de autoridades centralizadas creadas especialmente para este propósito. Como en relación con una red IP autónoma, asegurar la unicidad de los números de red y host puede lograrse mediante el administrador de la red.

En este caso, el administrador de la red tiene disponible todo el espacio de dirección, porque hacer coincidir direcciones IP en redes que no están conectadas no produciría efectos negativos. El administrador puede elegir de manera arbitraria direcciones porque es suficiente asegurar que las direcciones asignadas tienen la sintaxis correcta y garantizar que satisfacen las limitaciones enumeradas con anterioridad (que los números de red y host no puedan constar sólo de ceros o unos). Por cierto, el número de host en la tecnología TCP/IP es asignado de manera independiente de su dirección local.

Sin embargo, si se utiliza este enfoque, una red así será imposible de conectar a Internet en el futuro. Las direcciones elegidas de forma arbitraria pueden coincidir con direcciones de Internet asignadas centralmente. Para evitar conflictos de dirección ocasionados por tales coincidencias, los estándares de Internet han definido varias **direcciones privadas** que se recomiendan para uso autónomo:

- En la clase A: el número de red 10.0.0.0.
- En la clase B: un intervalo de 16 números de red: del 172.16.0.0 al 172.31.0.0.
- En la clase C: un rango de 255 números de red: del 192.168.0.0 al 192.168.255.0.

Estas direcciones se excluyen del conjunto de direcciones distribuidas centralmente y constan de un vasto espacio de dirección suficiente para numerar los hosts de redes de prácticamente cualquier tamaño. Las redes autónomas pueden utilizar las direcciones de estos intervalos. Nótese que pueden coincidir direcciones privadas en diferentes redes autónomas. Al mismo tiempo, utilizar direcciones privadas para redes autónomas permite conectarlas correctamente a Internet. Tecnologías especiales[1] utilizadas para este propósito eliminan las colisiones de dirección.

[1] La tecnología de traducción de dirección de red estudiada en el capítulo 20 es un ejemplo de una tecnología de este tipo.

17.4.2 Asignación de dirección centralizada

En redes grandes similares a Internet, la unicidad de las direcciones de red está asegurada por un sistema organizado jerárquicamente de manera centralizada de distribución de dirección. Puede asignarse un número de red sólo con la recomendación de una autoridad especializada de Internet. Desde 1998, la autoridad principal responsable del registro de direcciones globales de Internet es la **Corporación de Internet para Asignación de Nombres y Números (ICANN, Internet Corporation for Assigned Names and Numbers)**, organización no gubernamental y sin fines de lucro administrada por un consejo de directores. Esta organización controla la operación de departamentos regionales cuyas actividades abarcan vastas regiones geográficas: ARIN (para América), RIPE (para Europa) y APNIC (para la región Asia-Pacífico). Los departamentos regionales asignan bloques de dirección a grandes ISP, que a su vez los asignan a sus clientes, entre los cuales puede haber ISP más pequeños.

La escasez de direcciones de IP es el principal problema para su distribución centralizada. Por mucho tiempo, llegó a ser comparativamente difícil obtener una dirección de clase B y es casi imposible convertirse en propietario de una dirección de clase A. Esta escasez se debe no sólo al crecimiento de la red, sino también al uso poco eficaz del espacio de dirección disponible. Con bastante frecuencia, los propietarios de redes de clase C utilizan únicamente una pequeña parte de las 254 direcciones disponibles para ellos. Por ejemplo, considérese un ejemplo en el cual es necesario conectar dos redes mediante un enlace WAN. En tales casos se utilizan dos enrutadores conectados de acuerdo con el diseño "punto a punto" (figura 17.2). Para una red degenerada creada por el enlace que conecta los puertos de dos enrutadores adyacentes, es necesario asignar un número de red individual, aunque sólo se tengan dos nodos en una red de este tipo.

Para mitigar el problema de la escasez de direcciones, los diseñadores de la pila TCP/IP sugieren diversos enfoques. La solución más innovadora y radical consiste en idear una nueva versión de IP, IPv6, en la cual el espacio de dirección disponible se incremente de manera significativa con el uso de direcciones de 16 bytes. Sin embargo, incluso la versión IP actual, IPv4, soporta algunas tecnologías dirigidas a asegurar el uso más eficaz de las direcciones IP. Ejemplos de este tipo de tecnologías son NAT y CIDR.

17.4.3 Direccionamiento y CIDR

CIDR, establecida oficialmente en 1993 y estandarizada en RFC 1517, RFC 1518, RFC 1519 y RFC 1520, permite contar con centros de distribución de dirección para asignar cierto número de direcciones a sus suscriptores como sea necesario.

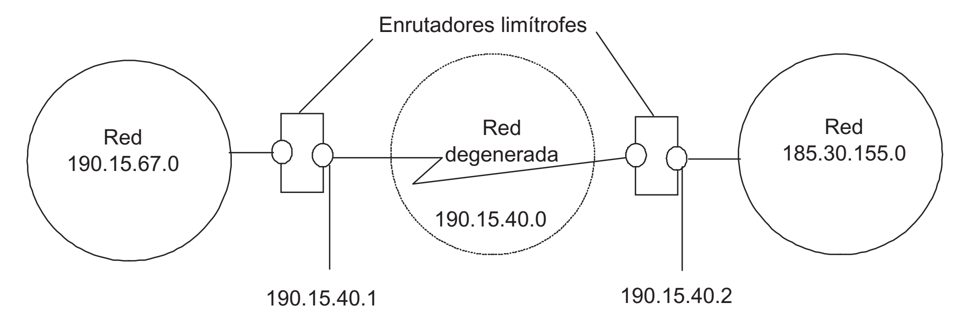


FIGURA 17.2 Uso ineficaz del espacio de dirección IP.

En la tecnología CIDR, una dirección IP se divide en un número de red y un número de host con base en una máscara de longitud variable más que a partir de uno o más bits más significativos, como era antes. Esta máscara de longitud variable se asigna al suscriptor mediante el proveedor de servicios. Para aplicar CIDR, la organización que administra las direcciones debe tener intervalos de dirección continuos. Tales direcciones tienen el mismo **prefijo** (es decir, los mismos valores de los diversos bits más significativos). Supóngase que algún proveedor de servicios tiene un espacio de dirección IP continuo de 2^n (figura 17.3). Por lo tanto, la longitud del prefijo es igual a $(32 - n)$ bits. Los n bits restantes desempeñan el papel del contador del número secuencial.

Cuando el cliente solicita a un proveedor de servicios asignar cierto intervalo de direcciones, el proveedor de servicios "recorta" el intervalo continuo S1, S2 o S3, según el número requerido de direcciones. Al mismo tiempo, se deben satisfacer los siguientes requerimientos:

- El número de direcciones en el área asignada debe ser igual a una potencia de dos.
- La frontera inicial del conjunto de dirección asignada debe ser múltiplo del número requerido de hosts.

El prefijo de cada área mostrada en la figura 17.3 tiene su propia longitud; cuanto más pequeño sea el número de direcciones en el área dada, más largo será su prefijo.

EJEMPLO *Supongamos que el ISP tiene un conjunto de direcciones que abarcan desde 193.20.0.0 hasta 193.23.255.255 (1100 0001.0001 0100.0000 0000.0000 0000 - 1100 0001.0001 0111.1111 1111.1111 1111). Esto significa que el número de direcciones a disposición de este ISP es de 218. Por consiguiente, el prefijo del ISP tiene la longitud de 14 bits, 1100 0001.0001 01 o, en otra forma, 193.20/14.*

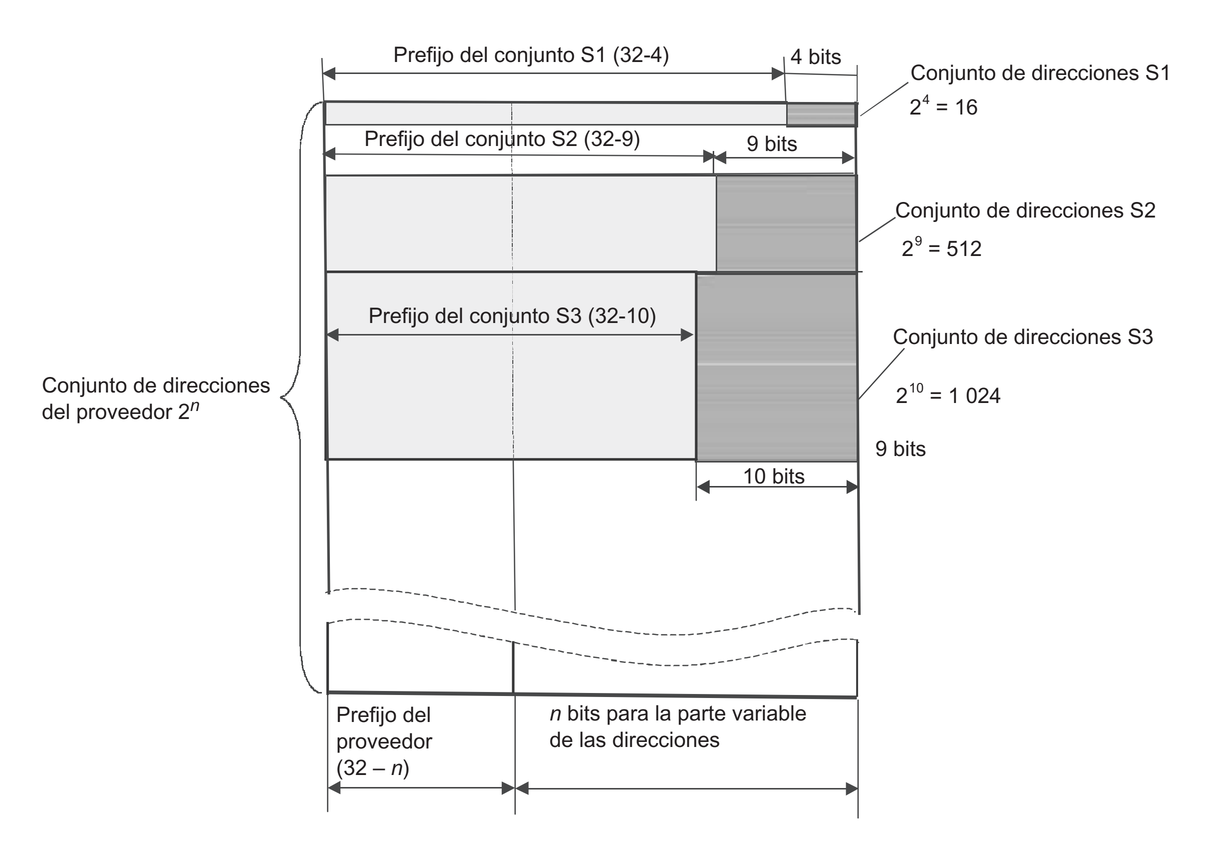


FIGURA 17.3 Distribución de direcciones con base en la tecnología CIDR.

Si un suscriptor de este ISP necesita un pequeño número de direcciones (por ejemplo, 13), el ISP podrá ofrecer a este suscriptor diversas variantes: la red 193.20.30.0/28, la red 193.20.30.16/28 o la red 193.21.204.48/28. En cualquiera de los casos, el suscriptor tiene los cuatro bits menos significativos a su disposición para numerar hosts de la red. De este modo, el número de nodos asignados para el suscriptor está expresado por el número mínimo que satisface los requerimientos del suscriptor (13), que pueden representarse mediante una potencia de dos ($2^4 = 16$). El prefijo para cada conjunto asignado en todos estos casos o del papel del número de redes tiene una longitud de 32 – 4 = 28 bits.

Ahora, considérese otra variante en la cual un gran cliente corporativo solicita servicio del ISP. Este cliente quizá planea proporcionar él mismo servicios de acceso a Internet. Supóngase también que dicho cliente requiere un bloque de dirección para 4 000 hosts. Para numerar una cantidad tan grande de hosts se requerirán 12 bits, lo que significa que el tamaño del conjunto de dirección asignado será algo mayor que el requerido: 4 096. La frontera antes de la cual el conjunto asignado debe iniciar debe ser múltiplo del tamaño del conjunto; éste puede ser cualquier dirección, como 193.20.0.0, 193.20.16.0, 193.20.32.0, 193.20.48.0, u otros números terminados en 12 ceros. Supóngase que el ISP ha ofrecido a este cliente el intervalo de dirección de 193.20.16.0 hasta 193.20.31.255. Para dicho intervalo, el número de red agregado (prefijo) tiene una longitud de 20 bits y es igual a 193.20.16.0/20.

Gracias a CIDR, el ISP tiene la posibilidad de "seccionar" bloques del espacio de dirección asignado a él de acuerdo con las necesidades y requerimientos de cada cliente.

En el capítulo 18 se reconsiderará la tecnología CIDR para explicar cómo ayuda a utilizar direcciones con moderación y a mejorar la eficacia del enrutamiento.

17.5 MAPEO DE DIRECCIONES IP A DIRECCIONES LOCALES

PALABRAS CLAVE: transmisión, dirección IP, dirección local, direcciones de mapeo, ARP, tabla de ARP, réplica de ARP, solicitudes ARP, caché de ARP, ARP Inverso y Proxy-ARP.

Uno de los problemas principales que tuvieron que resolverse cuando se creó IP fue asegurar la operación coordinada de la interred compuesta de varias redes constituyentes, las cuales por lo general utilizan diversas tecnologías de red. La interoperación de TCP/IP con tecnologías locales implementadas en una red constituyente tiene lugar muchas veces a medida que el paquete IP se envía a través de la interred. En cada enrutador, IP determina a cuál enrutador de esta red debería enviarse el paquete. Al resolver este problema, el protocolo determina la *dirección IP* de la interfase de red del siguiente enrutador (o el nodo terminal si esta red es la red de destino). Con el fin de aplicar la tecnología de la red local para liberar el paquete hacia el siguiente enrutador, es necesario llevar a cabo las siguientes operaciones:

1. Encapsular el paquete en la trama que tiene el formato correspondiente a esta red (por ejemplo, Ethernet).
2. Suministrar la trama con la *dirección local* del siguiente enrutador.

Como ya se ha mencionado,[2] todas estas tareas se delegan a nivel de la interfase de red de la pila TCP/IP.

[2] Véase la sección *"Pila TCP/IP"* en el capítulo 4.

17.5.1 ARP

Como no hay dependencia entre las direcciones locales y las direcciones IP, el único método para establecer mapeo es mediante el uso de tablas. Como resultado de la configuración de la red, cada interfase conoce su dirección local y su dirección IP. Se puede considerar que este mapeo es una tabla distribuida sobre interfases de red individuales. El único problema aquí es organizar el intercambio de esta información entre hosts de red.

Para definir la dirección local mediante la dirección IP, se utiliza el **protocolo de resolución de dirección (ARP**, por sus siglas para **Address Resolution Protocol)**. ARP es implementado de manera diferente según el protocolo de la capa de enlace de datos que funciona en la red local. Como el lector recordará, éste puede ser uno de los protocolos de LAN (Ethernet, Token Ring o FDDI), con la posibilidad de acceso de transmisión de todos los nodos de la red de manera simultánea o de uno de los protocolos WAN (X.25 o Frame Relay,) los cuales, como regla, no soportan el acceso de transmisión.

Considérese la operación ARP en LAN que soporten **transmisión**.

La figura 17.4 muestra este aumento de una red que incluye actos redes: Ethernet1 (incluidos tres nodos terminales, A, B y C) y Ethernet2 (incluidos los nodos terminales D y E). Estas redes se hallan conectadas a las interfases de enrutador 1 y 2, respectivamente. Cada interfase de red tiene una dirección IP y una dirección MAC. Supóngase que en algún caso, el módulo IP del host C envía un paquete hacia el host D. El protocolo del nodo C ha determinado la dirección IP del siguiente enrutador, IP_1. Antes de encapsular el paquete en la trama Ethernet y enviarlo hacia el enrutador, es necesario determinar su **dirección MAC** correspondiente. Para resolver este problema, IP solicita ARP, el cual soporta una **tabla ARP** por separado en cada interfase del enrutador o adaptador de red. En el curso de la operación de la red, esta tabla acumula información acerca de la correspondencia entre las direcciones IP y las direcciones MAC de otras interfases dentro de esta red. En un inicio, cuando la computadora o enrutador están conectados a la red, sus tablas ARP se encuentran vacías.

- En la figura 17.4, la etapa (1) corresponde al paso del mensaje siguiente desde IP hacia ARP: "¿qué dirección MAC corresponde a la interfase con la dirección de IP denotada IP_1?"
- La operación del ARP comienza con la consulta de la tabla alta de la interfase de red apropiada (etapa (2) en la figura 17.4). Supóngase que la dirección IP requerida no se encuentra entre los registros existentes.
- El paquete IP saliente para la cual fue imposible determinar la dirección local desde la tabla ARP es almacenado en el búfer o memoria temporal; ARP genera una solicitud, la encapsula en la trama Ethernet y la transmite [etapa (3) en la figura 17.4].
- Todas las interfases de la red Ethernet1 reciben esta solicitud de ARP y la dirigen a sus ARP "locales". ARP no sólo compara la dirección IP_1 especificada en el paquete con la dirección IP de la interfase a la cual llegó esta solicitud, sino también detecta una coincidencia (en este caso, el ARP se ejecuta en el enrutador 1) y formula una **réplica ARP** [etapa (4) en la figura 17.4].

En la réplica del ARP, el enrutador especifica su dirección local, MAC_1, y la envía hacia el nodo solicitante (en dicho ejemplo, éste será el nodo C) utilizando su dirección local. En tal caso, la réplica de transmisión no es necesaria, pues el formato de la solicitud ARP proporciona los campos para las direcciones local y de red del remitente. Obsérvese que el área dentro de la cual las solicitudes del ARP pueden propagarse está limitada por Ethernet1, pues el enrutador es una barrera para las tramas de transmisión.

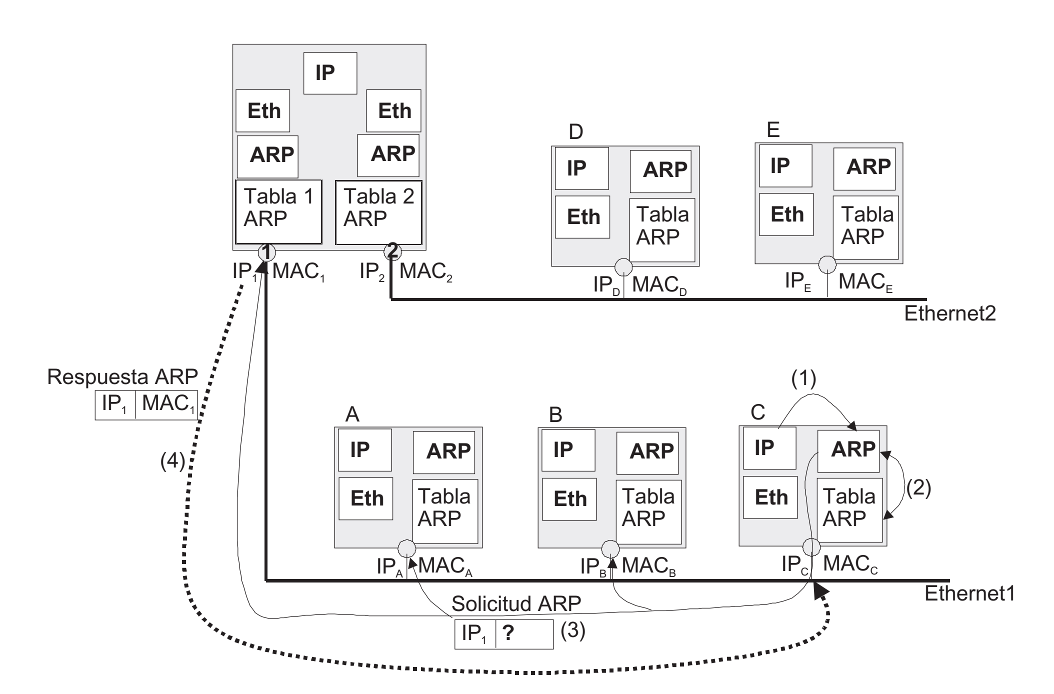


FIGURA 17.4 Método de operación ARP.

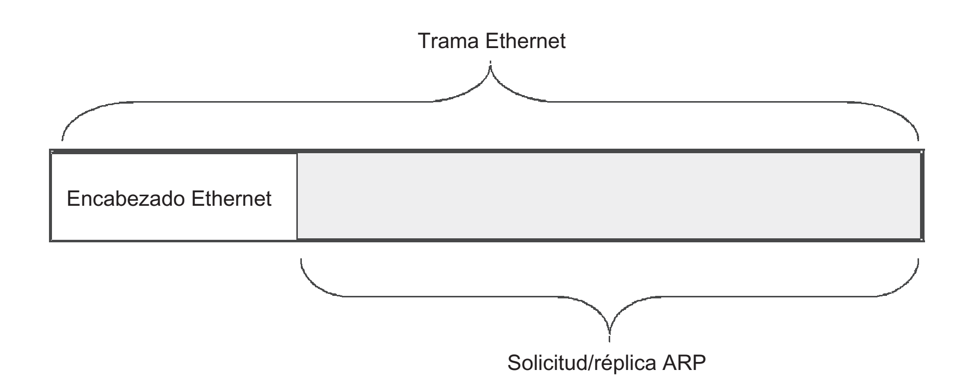


FIGURA 17.5 Encapsulación de un mensaje ARP en la trama Ethernet.

La figura 17.5 muestra la trama de Ethernet con un mensaje ARP encapsulado. La solicitud y réplica del ARP tienen el mismo formato. La tabla 17.2 enumera los valores de los campos de una solicitud ARP real que se pasa mediante el uso de Ethernet.

El campo *Network type* (*tipo de red*) contiene 1 para las redes Ethernet.

El campo *Protocol type* (*tipo de protocolo*) permite emplear ARP para IP y para otros protocolos de red. Para IP, este campo contiene el valor de 0x0800.

La longitud de la dirección local para el protocolo Ethernet es de 6 bytes, mientras que la longitud de la dirección IP es de 4 bytes. El campo *Operation* (*operación*) para solicitudes ARP contiene 1 si ésta es una solicitud y 2 si ésta es una réplica.

De esa solicitud se sigue que en la red Ethernet, el host con la dirección IP 194.85.135.75 intenta determinar la dirección MAC de otro host de la misma red, con la dirección IP 194.85.135.65. *El campo de la dirección local solicitada se llena con ceros.*

TABLA 17.2 Ejemplo de solicitud ARP

Tipo de red	1 (0x1)
Tipo de protocolo	2048 (0x800)
Longitud de dirección local	6 (0x6)
Longitud de dirección de red	4 (0x4)
Operación	1 (0x1)
Dirección local del remitente o emisor	008048B7E60
Dirección de red del remitente o emisor	194.85.135.75
Dirección local del receptor (la solicitada)	000000000000
Dirección de red del receptor	194.85.135.65

El host que ha reconocido su dirección IP envía una réplica a la solicitud. Si no hay computadora con la dirección IP solicitada en la red, no habrá réplica ARP. En este caso, IP descarta los paquetes IP enviados a esa dirección. La tabla 17.3 contiene los valores de los campos de la réplica de red que podrían enviarse a la solicitud ARP previamente proporcionada.

Al intercambiar estos dos mensajes ARP, el módulo de IP que ha enviado las solicitudes de la interfase con la dirección 194.85.135.75 ha determinado que la dirección MAC correspondiente a la dirección IP 194.85.135.65 es 00E0F77F1920. Esta dirección se colocará en el encabezado de la trama Ethernet que encapsula el paquete IP que espera para ser enviado.

Para reducir el número de mensajes ARP en la red, el mapeo detectado entre las direcciones IP y MAC se almacena en la tabla ARP de la interfase apropiada. En este caso, dicho registro aparecerá como sigue:

194.85.135.65 00E0F77F1920

TABLA 17.3 Ejemplo de réplica ARP

Tipo de red	1 (0x1)
Tipo de protocolo	2048 (0x800)
Longitud de dirección local	6 (0x6)
Longitud de dirección de red	4 (0x4)
Opción	1 (0x1)
Dirección local del remitente o emisor	00E0F77F1920
Dirección de red del remitente o emisor	194.85.135.65
Dirección local del receptor (la solicitada)	008048EB7E60
Dirección de red del receptor	194.85.135.75

Se agrega un nuevo registro de manera automática a la tabla varios milisegundos después que el módulo ARP completa su análisis de la réplica ARP. Ahora, si debe enviarse de nuevo un paquete hacia la dirección 194.85.135.65, IP verificará si esta dirección aparece en la tabla ARP antes de enviar una solicitud de transmisión.

La tabla ARP se ve suplementada no sólo por la réplica ARP que llega a la interfase para la cual ha sido creada, sino también como resultado de recuperar información útil de las solicitudes ARP de transmisión. De hecho, como se observa en las tablas 17.2 y 17.3, cada solicitud contiene las direcciones IP y de las direcciones MAC del remitente. Todas las interfases que han recibido esta solicitud pueden colocar información acerca de la dirección local a la red mapeada del remitente a sus propias tablas ARP. En particular, todos los hosts que han recibido la solicitud ARP mostrada en la tabla 17.2 pueden colocar el registro siguiente en sus tablas ARP:

194.85.135.75 008048EB7E60

Así, una tabla ARP complementada por los dos registros mencionados durante la operación de la red aparecerá como se muestra en la tabla 17.4.

TABLA 17.4 Ejemplo de tabla ARP

Dirección IP	Dirección MAC	Tipo de registro
194.85.135.65	00E0F77F1920	Dinámico
194.85.135.75	008048EB7E60	Dinámico
194.85.60.21	008048EB7567	Estático

El campo *Record type* (*tipo de registro*) puede contener uno de los siguientes valores: *estático* o *dinámico*. Los registros estáticos se crean en forma manual por medio de la utilidad ARP y no tienen término de expiración. Para ser más precisos, existen hasta que la computadora o el enrutador son apagados.

Los registros dinámicos son creados por el módulo ARP al emplear las capacidades de transmisión de las tecnologías LAN. La tabla ARP está complementada mediante el análisis de las réplicas ARP que llegan a la interfase actual y al recuperar información útil de las solicitudes ARP de transmisión. Como es evidente de la tabla 17.2, las solicitudes ARP, aparte de otros datos, contienen las direcciones IP y MAC del remitente. Incluso si no hay coincidencia con la dirección solicitada, el host coloca esta valiosa información en su propia tabla ARP.

Los registros dinámicos deben renovarse (o “refrescarse”) de manera periódica. Si el registro no fue actualizado durante un tiempo predeterminado (varios minutos), se descartará de la tabla. De este modo, las tablas ARP almacenan registros en hosts de red que participan de manera activa en las operaciones de la red más que en todos los hosts de la red. Dado que un método de esta naturaleza para almacenamiento de información es conocido como caché, una tabla ARP se conoce a menudo como **caché de ARP**.

NOTA *Algunas implementaciones de IP y ARP no colocan paquetes IP en la cola por el tiempo requerido para esperar réplicas ARP. En vez de ello, simplemente descartan los paquetes IP y delegan la tarea de su restauración al módulo TCP o el proceso de aplicación y funcionan a través de UDP. Una restauración de esta clase utiliza tiempos de descanso y un mecanismo de retransmisión. La retransmisión del mensaje se llevará a cabo con éxito, pues el primer intento ya habría actualizado la tabla ARP.*

El método de resolución de dirección utilizado en las WAN es diferente. Como se recordará, las WAN no soportan mensajes de transmisión. En este caso, el administrador de la red debe crear de forma manual las tablas ARP y colocarlas en uno de los servidores. Estas tablas ARP especifican, por ejemplo, el mapeo de direcciones IP a direcciones X.25, las cuales se interpretan como direcciones locales por IP. En las WAN también existe una tendencia a automatizar ARP. Para este propósito, se elige un enrutador dedicado de todos los enrutadores conectados a una WAN. Este enrutador soporta la tabla ARP para los otros hosts y enrutadores de esa red.

Cuando se utiliza un enfoque centralizado de esa forma, para todos los hosts y enrutadores, solamente es necesario especificar de modo manual las direcciones IP y la dirección local del enrutador dedicado. Cuando se activan, cada host y enrutador registran sus direcciones en el enrutador dedicado. Se requiere algún tiempo para determinar la dirección local de una dirección IP, el módulo ARP solicita el enrutador dedicado y tiene automáticamente una réplica, sin la participación del administrador. Un enrutador ARP que funciona de tal manera se conoce como *servidor ARP*.

En algunos casos, tiene que resolverse un problema inverso: determinar la dirección IP a partir de la dirección local conocida. En este caso, se utiliza el *protocolo de resolución de dirección inverso* (*Reverse ARP o RARP*), el cual se utiliza, por ejemplo, cuando se inician las estaciones de trabajo sin unidad de disco que al inicio no conocen sus direcciones IP pero sí la dirección MAC del adaptador de red.

17.5.2 Proxy-ARP

Proxy-ARP es una de las variantes del ARP que permite mapear las direcciones IP a direcciones de hardware en redes que soportan transmisión, incluso cuando el host solicitado se localiza fuera de las fronteras del dominio de colisión actual.

La figura 17.6 muestra una red con un nodo terminal (computadora D) que funciona en el modo de host remoto. Se proporcionarán más detalles acerca de este modo de funcionamiento en el capítulo 23 de la parte V; por el momento, es suficiente saber que la operación o funcionamiento del nodo terminal en modo de esta clase tiene todas las posibilidades disponibles para computadoras localizadas dentro de la parte principal de la Ethernet. Entre otras características, tiene la dirección IP, IP_D, perteneciente a la misma red. Para todos los nodos terminales de la Ethernet, las características específicas de conexión de un host remoto (la presencia de módems, conexión a redes por línea telefónica y PPP) son transparentes e interactúan de manera normal con un host de esta clase. Para hacer posible un modo de operación así, entre otras características, se requiere Proxy-ARP. Como el host remoto está conectado con PPP, no tiene dirección MAC.

Supóngase que la aplicación ejecutada en la computadora C decide enviar un paquete a la computadora D. Aunque se conoce la dirección IP de destino, IP_D, como ya se mencionó, para transmitir un paquete mediante Ethernet, es necesario encapsular ese paquete en la trama de Ethernet y suministrarlo con la dirección MAC. Para determinar la dirección MAC de la computadora D, la IP de la computadora C solicita ARP, lo cual envía un mensaje de transmisión que contiene una solicitud ARP. Si no hubiera instalación para Proxy-ARP en un enrutador, ningún host contestaría esta solicitud.

No obstante, Proxy-ARP está instalado y funciona de la siguiente manera: cuando el host D remoto se conecta a la red, el registro siguiente es introducido en la tabla ARP del enrutador:

$$IP_D — MAC_1 — int2$$

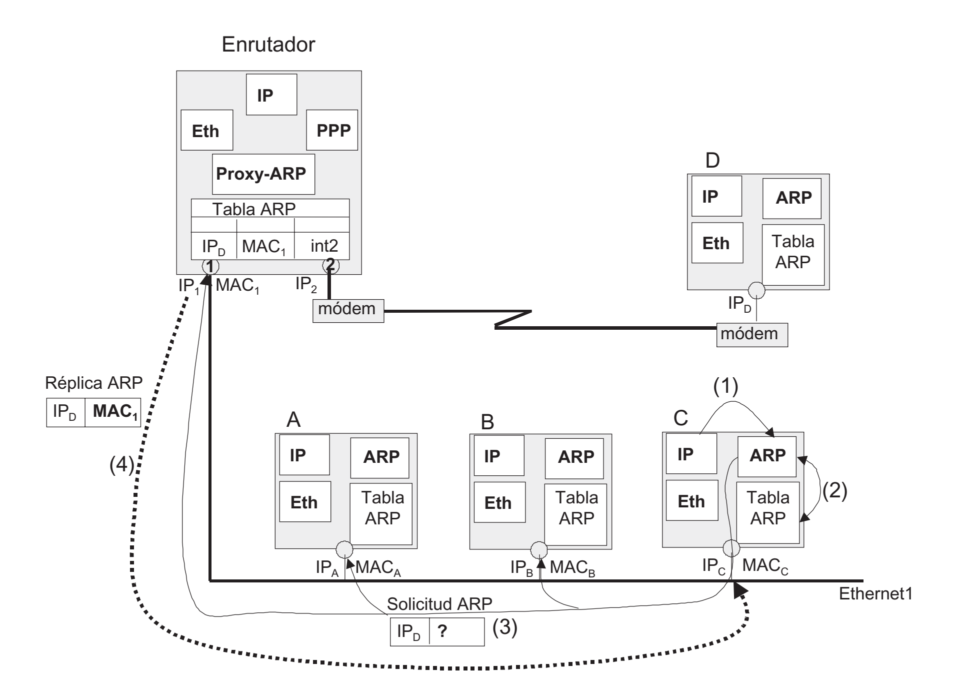


FIGURA 17.6 Método de operación Proxy-ARP.

Este registro tiene el significado que sigue:

- Cuando llega la solicitud ARP en referencia a la dirección IP_D, la réplica ARP debe suministrarse con la dirección de hardware MAC_1 correspondiente a la dirección de hardware de la interfase 1 del enrutador.
- El host con la dirección IP_D está conectado a la segunda interfase del enrutador.

Por lo tanto, el enrutador con Proxy-ARP instalado contestará la solicitud de transmisión enviada por el host C. El enrutador coloca una réplica ARP "proxy" en la cual suministra su propia dirección de hardware MAC_1 en lugar de la de la computadora D.

El host C, sin sospechar ningún "truco", envía la trama con el paquete IP encapsulado hacia la dirección MAC_1. Una vez recibida la trama, el Proxy-ARP "comprende" que ésta no se ha destinado a él, pues el paquete contiene la dirección IP de otro host. En consecuencia, la dirección de destino debe buscarse en la tabla ARP. La consulta de la tabla muestra que la trama debe enviarse al host conectado a la segunda interfase.

El método anterior es el más simple del uso de Proxy-ARP; no obstante, refleja la lógica de la operación con suficiente detalle.

17.6 DNS

PALABRAS CLAVE: nombres privados, nombres relativos, nombres de dominio completamente calificados (FDQN, Fully Qualified Domain Names), nombres simbólicos simples, nombres simbólicos jerárquicos, nombres NetBIOS, servidores DNS, clientes DNS, base de datos distribuida, método recursivo, método iterativo y zona de consulta inversa.

17.6.1 Nombres simbólicos simples

En sistemas operativos diseñados inicialmente para que funcionen en LAN, como Novell NetWare, Microsoft Windows o IBM OS/2, los usuarios siempre utilizaban los nombres simbólicos de computadoras. Como las LAN constan de pequeños números de computadoras, se empleaban *nombres simples*, que representaban cadenas de texto no divididas en partes. Ejemplos de tales nombres son NW1_1, mail2 y LONDON_SALES_2. Para establecer el mapeo de nombres simbólicos a direcciones MAC, estos sistemas operativos empleaban mecanismos de solicitudes de transmisión, semejantes al utilizado por ARP. Por ejemplo, el mecanismo de resolución del nombre de transmisión se ha puesto en marcha en el protocolo Net-BIOS, que sirve como base para muchos sistemas operativos de LAN. Los así denominados nombres Net-BIOS han servido como un tipo principal de nombres simples en LAN por años.

Para la pila TCP/IP, por lo general destinada para funcionar en grandes redes distribuidas geográficamente, un enfoque así demostró ser ineficaz.

17.6.2 Nombres simbólicos jerárquicos

La pila TCP/IP utiliza DNS, que tiene una estructura jerárquica que permite usar un número arbitrario de componentes en un nombre (figura 17.7).

La jerarquía de los nombres de dominio es semejante a la de nombres de archivo adoptados en los sistemas de archivos más conocidos. El árbol de nombres comienza desde la raíz, designada aquí por el punto (.), la cual es seguida de la parte simbólica más significativa del nombre, luego la siguiente parte más significativa del nombre y así sucesivamente. La parte menos significativa del nombre corresponde al nodo terminal de la red. En contraste con un nombre de archivo, en el cual el componente más significativo aparece primero, seguido del componente del nivel inferior y así sucesivamente, un nombre de dominio comienza

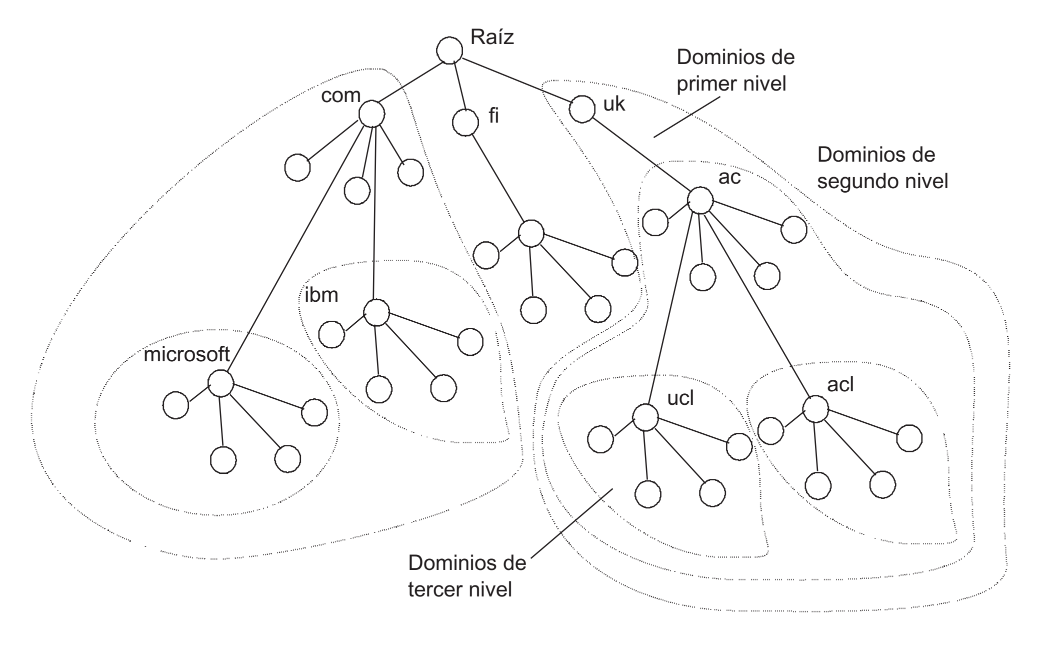


FIGURA 17.7 Espacio de nombres de dominio.

con los componentes menos significativos y es exterminado por el componente de más alto nivel. Los componentes de un nombre de dominio están delimitados mediante puntos. Por ejemplo, en **partnering.microsoft.com**, el componente **partnering** es el nombre de una de las computadoras en el dominio **microsoft.com**.

La división de nombres en partes no sólo divide las responsabilidades administrativas para asignación de nombres únicos, sino también los divide entre varios individuos u organizaciones dentro de los límites específicos de la jerarquía. De este modo, en el ejemplo proporcionado en la figura 17.7, es posible delegar las responsabilidades para asegurar que todos los nombres terminados por el componente "us" proporcionen la parte única del nombre de la capa de jerarquía inferior a un individuo. Si ese individuo es capaz de sostener esa responsabilidad, todos los nombres (como **www.us, mail.mmt.us** o **m2.zil.mmt.us**) diferirán en su segunda parte de acuerdo con su significancia.

La separación de las responsabilidades administrativas resuelve el problema de generar nombres únicos sin necesidad de coordinar esfuerzos entre varias organizaciones responsables de los nombres del mismo nivel jerárquico. Obviamente, debe haber una organización responsable de la asignación de los nombres del nivel jerárquico superior.

El conjunto de nombres con las mismas partes más significativas que comprenden uno o más componentes conforman un dominio. Por ejemplo, nombres como **www1.zil.mmt.ru**, **ftp.zil.mmt.ru**, **yandex.ru** y **s1.mgu.ru** son parte del dominio **ru**, pues todos estos nombres tienen en común la parte más significativa del nombre: **ru**. Otro ejemplo es el dominio **mgu.ru**. Entre los nombres de la figura 17.8, los siguientes forman parte de este dominio: **s1.mgu.ru, s2.mgu.ru** y **m.mgu.ru**. Dicho dominio consta de los nombres para los cuales las dos partes más significativas son siempre **mgu.ru**. El administrador del dominio **mgu.ru** es responsable de la unicidad de los nombres del siguiente nivel, los cuales pertenecen al dominio, por ejemplo; nombres como **s1**, **s2** y **m**. Los subdominios resultantes **s1.mgu.ru, s2.mgu.ru** y **m.mgu.ru** son subdominios del dominio **mgu.ru,** porque tienen la parte más significativa del nombre en común. Para abreviar, los subdominios suelen ser llamados por la parte menos significativa del nombre: **s1**, **s2** y **m**.

NOTA *El término dominio tiene diversos significados; por lo tanto, siempre debe interpretarse dentro de un contexto específico. Aparte de los nombres de dominio de la pila TCP/IP, la terminología relacionada con computación hace referencia a los dominios de Windows NT, dominios de colisión y así sucesivamente. La característica común de estos conceptos de dominio es que todos describen algún conjunto de computadoras caracterizadas por un rasgo específico en común.*

Si la unicidad de los nombres del siguiente nivel de la jerarquía está asegurada en cada dominio o subdominios, todo el sistema de nombres consistirá en nombres únicos.

Por analogía con el sistema de archivos, DNS proporciona *nombres cortos*, *nombres relativos* y *nombres de dominio completamente calificados* (*FQDN,* por las siglas para *Fully Qualified Domain Names*). Un nombre corto es aquel del nodo terminal de la red, como el puerto del enrutador o del host. El nombre corto representa una hoja del árbol de nombres. Un nombre relativo es el nombre compuesto que comienza desde algún nivel jerárquico (sin embargo, no desde el nivel superior). Por ejemplo, **www1.zil** es un nombre relativo. Un FQDN incluye los componentes del nombre de todos los niveles de la jerarquía a partir del nombre corto y termina con la raíz: **www1.zil.mmt.ru**.

Un dominio raíz es administrado por autoridades centralizadas de Internet: IANA e InterNIC. Los dominios de nivel superior son asignados para cada país, además de sobre una base centralizada. Los nombres de estos dominios deben seguir el estándar internacional ISO

3166. Se utilizan abreviaturas de dos o tres letras para designar los países, por ejemplo: us (United States, Estados Unidos), ru (Rusia), uk (United Kingdom, Reino Unido de la Gran Bretaña) o fi (Finlandia). Para distintas clases de organizaciones, existen las abreviaturas siguientes:

- **com:** organizaciones comerciales (por ejemplo, **microsoft.com**)
- **edu:** organizaciones educativas (por ejemplo, **mit.edu**)
- **gov** (o **gob**)**:** organizaciones de gobierno (por ejemplo, **nsf.gov**)
- **org:** organizaciones sin fines de lucro (por ejemplo, **fidonet.org**)
- **net:** organizaciones que soportan redes (por ejemplo, **nsf.net**)

Cada dominio está administrado por una organización individual que suele dividir su dominio en subdominios y delega las funciones administrativas para estos subdominios a otras organizaciones. Para obtener el nombre del dominio, es necesario registrarlo con una organización específica a la cual InterNIC haya delegado los derechos para distribuir nombres de dominio.

IMPORTANTE *Las computadoras se encuentran incluidas en dominios de acuerdo con sus nombres completamente calificados. Al mismo tiempo, pueden tener direcciones IP independientes que pertenezcan a redes y subredes diferentes. Por ejemplo, el dominio* ***mgu.ru*** *puede incluir hosts con direcciones tales como 132.13.34.15, 201.22.100.33 y 14.0.0.6.*

DNS se encuentra instalado en Internet; no obstante, también puede funcionar como un sistema de nombres autónomo en cualquier red corporativa extendida que utilice la pila TCP/IP pero que no esté conectada a Internet.

17.6.3 Modo de operación DNS

El método de transmisión para establecer el mapeo de nombres simbólicos y direcciones locales, semejante al ARP, funciona de manera eficaz solamente en una LAN pequeña que no se encuentre dividida en subredes. En redes a gran escala, donde no se soporta la transmisión ilimitada, se necesita otro método de resolución de nombres simbólicos. El uso de un servicio centralizado que soporte el mapeo entre direcciones de diferentes tipos para todas las computadoras de la red es una buena alternativa a la transmisión. Por ejemplo, Microsoft puso en marcha el servicio centralizado WINS para su sistema operativo corporativo Windows NT. El servicio WINS soporta la base de datos de NetBIOS y direcciones IP correspondientes a ellos.

El mapeo entre los nombres de dominio y la direcciones IP en redes TCP/IP puede establecerse mediante el uso de herramientas del host local y del servicio *centralizado*.

En las etapas iniciales de la evolución de Internet, un archivo del texto nombrado hosts. txt tenía que crearse de forma manual en cada host. Este archivo contenía cierto número de redes, cada una con un par de "dirección IP - nombre de dominio", por ejemplo, 102.54.94.97: **rhino.acme.com**.

Con el crecimiento de Internet crecieron los archivos de hosts. Por lo tanto, el desarrollo de una solución escalable para resolver los nombres se convirtió en una necesidad. DNS llegó a ser esa solución.

DNS es un servicio centralizado fundamentado en la base de datos distribuida de mapeo entre nombres de dominio y direcciones IP. En su operación, DNS utiliza el protocolo cliente-servidor, el cual define los servidores DNS y los clientes DNS. Los servidores DNS soportan la base de datos distribuida de mapeos, mientras que los clientes DNS solicitan servidores para resolver los nombres de dominio para direcciones IP.

El servicio DNS usa archivos de texto con un formato semejante al del archivo de host. Estos archivos los prepara de forma manual el administrador de la red; sin embargo, el servicio DNS depende de la jerarquía de dominios y cada servidor del servicio DNS almacena únicamente parte de los nombres de red en vez de todos ellos, como se hacía con los archivos de host. A medida que el número de hosts dentro de la red se incrementa, el problema de escalamiento se resuelve al crear nuevos dominios y subdominios y mediante la adquisición de nuevos servidores DNS.

Para cada dominio de nombres, debe generarse un servidor DNS. Existen dos métodos de distribución de nombres en servidores. En el primer caso, el servidor puede almacenar el mapeo de "nombre de dominio-dirección IP" para todo el dominio, incluidos todos sus subdominios. Sin embargo, tal solución es poco escalable, pues a medida que se agregan nuevos subdominios, la carga en este servidor puede exceder sus capacidades. Por consiguiente, se usa con más frecuencia otro enfoque. Cuando se utiliza este enfoque, el servidor de nombres almacena sólo los nombres que terminan en el siguiente nivel inferior de jerarquía, en vez del nombre del dominio. Este enfoque es similar al utilizado por los directorios de sistemas de archivos, los cuales contienen registros en los archivos y los subdirectorios dentro de ellos. Cuando se aplica este método para organizar el servicio DNS, la carga se distribuye de modo uniforme entre todos los servidores DNS de la red. Por ejemplo, en el primer caso, el servidor DNS del dominio **mmt.ru** almacena los mapeos para todos los nombres con terminación en **mmt.ru**: **www1.zil.mmt.ru**, **ftp.zil.mmt.ru**, **mail.mmt.ru** y así sucesivamente. En el segundo caso, este servidor almacena los mapeos sólo para nombres como **mail.mmt.ru**, **www.mmt.ru** y así de forma progresiva; todos los otros mapeos deben almacenarse en el servidor DNS del subdominio **zil**.

Aparte de la tabla de mapeo, cada servidor DNS contiene los enlaces a los servidores DNS de sus subdominios, enlaces que conectan a servidores SNS separados en el servicio unificado DNS. Las referencias son direcciones IP de los servidores correspondientes. Para servir el dominio raíz, están dedicados servidores DNS alternativos, cuyas direcciones IP son bien conocidas (por ejemplo, sus listas pueden obtenerse de InterNIC).

El procedimiento para resolver un nombre DNS es similar en muchos aspectos al procedimiento de búsqueda de una dirección de archivo en el sistema de archivos, dado su nombre simbólico. En ambos casos, el nombre completamente calificado refleja las estructuras jerárquicas de la organización de las tablas de referencia apropiadas: directorios de archivos y tablas DNS, respectivamente. Aquí el dominio y su servidor DNS son un análogo del sistema de archivos. De manera semejante a los nombres de archivo simbólicos, los nombres de dominio están caracterizados por la independencia de nombres de una ubicación física.

El procedimiento de búsqueda para una dirección de archivo mediante su nombre simbólico consiste buscar de forma secuencial todos los directorios, a partir de la raíz. En este caso, se examinan primero el caché y el directorio actuales. Para definir la dirección IP mediante su nombre de dominio, también es necesario consultar todos los servidores DNS que forman una cadena de subdominios incluidos dentro del nombre del host, comenzando desde el dominio raíz. La diferencia más considerable entre la búsqueda en el sistema de

archivos y la búsqueda DNS es que un sistema de archivos se encuentra localizado en una sola computadora, mientras que DNS está distribuido.

Existen dos métodos para resolver nombres DNS. En el primer caso, el cliente DNS coordina el trabajo relacionado con la búsqueda de la dirección IP:

- El cliente DNS solicita el servidor DNS raíz y especifica el FQDN.
- El servidor DNS responde al especificar la dirección del siguiente servidor DNS que sirve al dominio de nivel superior especificado en la parte más significativa del nombre solicitado.
- El cliente DNS solicita el siguiente servidor DNS, el cual lo redirige al servidor DNS del subdominio requerido, y así sucesivamente. Este procedimiento continúa hasta que se encuentra el servidor DNS requerido que contiene el mapeo para el nombre solicitado hacia una dirección específica. Este servidor envía la réplica final hacia el cliente.

Este método de interacción se conoce como **método no recursivo** o **método iterativo**. En este caso, el cliente realiza de forma iterativa una secuencia de solicitudes a diferentes servidores de nombres. Este método se usa rara vez, porque deja al cliente la carga de tareas más complicadas.

La segunda variante implementa el **procedimiento recursivo**:

- El DNS solicita el servidor DNS local (por ejemplo, el que sirve en su dominio al que pertenece el nombre del siguiente).
- Si el servidor DNS local conoce la respuesta, de inmediato la devolverá al cliente. Esto puede ocurrir cuando el nombre solicitado es parte del mismo subdominio que el cliente. También esto puede corresponder a un servidor que ya ha realizado esta solicitud para otro cliente y lo ha almacenado en su caché.
- Si el servidor local no sabe la respuesta, efectuará solicitudes interactivas al servidor raíz como lo hizo el cliente en la primera variante. Una vez recibida una respuesta, el servidor DNS la envía al cliente, el cual durante la ejecución de la solicitud simplemente espera por una respuesta desde su servidor DNS local.

En este método, el cliente delega los procedimientos a su servidor. Por lo tanto, este método se conoce como indirecto o recursivo. Casi todos los clientes DNS utilizan un procedimiento recursivo.

Para acelerar el procedimiento de la búsqueda de direcciones IP, los servidores DNS utilizan con amplitud el procedimiento de caché para todas las respuestas que pasan a través de ellos. Con el fin de habilitar el servicio DNS para procesar los cambios que tienen lugar en la red de manera oportuna, las respuestas se guardan en caché durante un tiempo más o menos corto, que suele ser desde algunas horas hasta varios días.

17.6.4 Zona de consulta inversa

El servicio DNS está proyectado no sólo para encontrar direcciones IP mediante nombres de host, sino también para resolver un **problema inverso**: encontrar nombres de host mediante direcciones IP conocidas.

La mayoría de los programas y utilidades que usan el DNS tratan de encontrar el nombre de host mediante su dirección cuando el usuario ha especificado sólo la dirección o cuando esa dirección es recuperada desde el paquete que el programa recibió proveniente de la red. Los registros inversos no necesariamente existen, incluso para las direcciones que tienen registros directos. Los administradores pueden tan sólo olvidar crearlos. En ocasiones, la

creación de tales registros requiere un pago extra, en especial si el servidor primario de la zona de consulta inversa está soportado por un ISP. Cuando no hay zona de consulta inversa, dichos programas funcionan con repartos significativos, pues tienen que esperar largo tiempo por las solicitudes inversas.

Por consiguiente, un problema inverso es solucionado en Internet al organizar las denominadas *zonas de consulta inversa*.

Una **zona de consulta inversa** es el conjunto de tablas que almacenan el mapeo entre las direcciones IP de alguna red y los nombres de hosts pertenecientes a la misma red. Con el fin de organizar un servicio distribuido y utilizar el mismo software para buscar nombres y direcciones, la dirección IP compuesta es considerada en el mismo estilo que el nombre compuesto.

Por ejemplo, se estima que una dirección como 192.31.106.0 contiene la parte más significativa correspondiente al dominio 194, seguida del dominio 31, el cual incluye el dominio 106. Para almacenar el mapeo de todas las direcciones que comienzan con 192, se crea la zona 194 con sus servidores de nombres primarios y secundarios. Cuando se escribe una dirección, la parte más significativa de la dirección es la que se encuentra más al extremo izquierdo; para nombres, la situación es la opuesta. Por lo tanto, para obtener completa correspondencia en una solicitud inversa, la dirección se especifica en el orden inverso (por ejemplo, 106.31.192 para el ejemplo proporcionado anteriormente).

Para registros en los servidores que controlan las zonas de consulta inversa de nivel superior se crea una zona especial: in-addr.arpa. Por consiguiente, el registro completo para dirección utilizada en este ejemplo tiene el aspecto siguiente:

106.31.192.in-addr.arpa.

Los servidores primarios para las zonas de consulta inversa utilizan los archivos de las bases de datos independientes de los archivos de las zonas principales, donde existen registros sobre el mapeo directo de los mismos nombres y direcciones. Tal organización puede producir discordancia, pues el mismo mapeo se introduce en los archivos dos veces.

17.7 DHCP

PALABRAS CLAVE: protocolo de configuración de host dinámico (DHCP), servidor DHCP, cliente DHCP, direcciones estáticas, direcciones dinámicas, modo automático/manual, asignación de direcciones, duración de arrendamiento y DNS dinámico.

Para la operación normal de la red, cada interfase de red de una computadora o enrutador que enviará o recibirá paquetes IP debe tener asignada una dirección IP.

La asignación de direcciones IP puede llevarse a cabo de forma manual en el curso de la configuración de la interfase. Para computadoras, este procedimiento consiste en llenar una serie de diálogos que se exhiben en pantalla. Cuando se procede de esta manera, el administrador debe recordar cuáles direcciones del conjunto disponible se encuentran asignadas a otras interfases y cuáles están libres.

El **protocolo de configuración de host dinámico (DHCP)** automatiza el proceso de configurar las interfases de redes y asegura eliminar la duplicación de direcciones mediante el uso de la base de datos de direcciones administrada de forma central. La operación del DHCP se describe en RFC 2131 y RFC 2132.

17.7.1 Modos DHCP

DHCP funciona de acuerdo con el modelo cliente-servidor. En el inicio del sistema, un cliente DHCP envía una solicitud de transmisión hacia la red y solicita que se le asigne una dirección IP. El servidor DHCP responde a esta solicitud y envía un mensaje de respuesta que contiene una dirección IP y otros parámetros de configuración.

El servidor DHCP puede funcionar en varios módulos:

- Asignación manual de direcciones estáticas.
- Asignación automática de direcciones estáticas.
- Distribución automática de direcciones dinámicas.

En todos los modos de funcionamiento u operación, el administrador configura el servidor DHCP y especifica uno o más intervalos de direcciones IP para él. Todas estas direcciones deben relacionarse con la misma red (es decir, deben tener el mismo valor en el campo el número de red).

En el *modo manual*, el administrador, aparte de proporcionar el conjunto de direcciones disponibles, suministra al servidor DHCP la información que define estrictamente el mapeo de las direcciones IP a las direcciones físicas u otros identificadores de los nodos del cliente. Con esta información, el servidor DHCP siempre asigna la misma dirección IP predefinida al cliente DHCP con conjunto de otros parámetros de configuración.[3]

En el modo de *asignación automática de direcciones estáticas*, el servidor DHCP elige de manera arbitraria una dirección IP para el cliente sin la participación del administrador. Esta dirección es seleccionada del conjunto de direcciones IP disponibles. Una dirección del conjunto se asigna al cliente de modo constante, lo cual significa que existe un mapeo constante entre la dirección IP del cliente y su información de identificación, como era el caso con la asignación manual. Este mapeo se establecía cuando el servidor DHCP asignaba la dirección IP al cliente por primera vez. Todas las solicitudes adicionales del cliente para la asignación de una dirección IP devuelven la misma dirección IP desde el servidor DHCP.

Cuando se utiliza *distribución dinámica de direcciones*, el servidor DHCP asigna direcciones IP a sus clientes por un tiempo limitado, conocido como **duración de arrendamiento**. Si una computadora que es un cliente DHCP se elimina de la red, la dirección IP asignada a la misma se liberará automáticamente. Cuando la computadora se conecta a otra subred, se le asignará de forma automática una nueva dirección. Ni el usuario final ni el administrador de la red participan en este proceso.

La distribución automática de direcciones proporciona la posibilidad de usar de nuevo en un futuro la dirección IP liberada mediante la asignación de la misma a otra computadora. De este modo, aparte de la ventaja principal de DHCP en la automatización del trabajo administrativo de rutina para configurar la pila TCP/IP en cada computadora, la asignación dinámica de dirección permite construir redes IP en las que el número de nodos excede el número de direcciones IP disponibles.

EJEMPLO *Considérense las ventajas proporcionadas por la distribución dinámica del conjunto de direcciones en el ejemplo de una compañía cuyos empleados gastan la mayor parte de su tiempo de trabajo fuera de la compañía trabajando desde el hogar o durante los viajes de negocios. Cada empleado tiene una computadora portátil conectada a la red IP corporativa cuando trabaja en la compañía. Debe contestarse una pregunta: ¿cuántas direcciones IP son necesarias para una compañía de esta naturaleza?*

---

[3] En ocasiones se omitirá esta especificación por brevedad.

La primera respuesta sería la siguiente: el número de direcciones debe ser igual a la cantidad de empleados que trabajan en la red. Por ejemplo, si existen 500 de estos empleados, cada uno de ellos deberá tener asignados una dirección IP y un lugar de trabajo. De esta manera, la administración debe solicitar al ISP las direcciones de dos redes de clase C y equipar los locales. Sin embargo, recuérdese que los empleados de esta empresa rara vez visitan las oficinas principales. Por consiguiente, la mayor parte del tiempo no se utilizarán dichos recursos si se elige una solución de esta naturaleza.

Otro enfoque consiste en solicitar un número de direcciones IP que corresponda a la cantidad de empleados que se encuentran normalmente en la compañía (con alguna reserva). Por ejemplo, si el número normal de empleados en la oficina no excede de 50, será suficiente solicitar un conjunto de 64 direcciones e instalar una red con 64 conectores para enchufar las computadoras. Sin embargo, surge otro problema: ¿quién y cómo configuraría las computadoras que se agregarían o removerían constantemente de la red?

Existen dos maneras de resolver este problema. La primera, el administrador (o un usuario móvil) puede configurar de forma manual la computadora cuando sea necesario para conectarla a la red de la compañía. Este enfoque requiere un gran número de operaciones de rutina; en consecuencia, ésta no es una buena solución. En una situación así, la posibilidad de asignar de manera automática direcciones DHCP parece mucho más atractiva. Si se utiliza este enfoque, el administrador podrá especificar un intervalo de 64 direcciones cuando tenga que configurar el servidor DHCP. Después de esto, cada nuevo usuario móvil que llegue sólo conectará físicamente su computadora a la red y se iniciará el cliente DHCP; a su vez, éste solicita los parámetros de configuración requeridos y los recibe automáticamente desde el servidor DHCP. De esa manera, para soportar 500 usuarios móviles, es suficiente tener 64 direcciones IP y 64 lugares de trabajo en la red de la compañía.

17.7.2 Algoritmo de asignación de dirección dinámica

Un administrador controla el proceso de configuración de la red al especificar los dos parámetros principales de la configuración de servidor DHCP: el conjunto de direcciones disponibles para distribución y la duración del arrendamiento. La duración de arrendamiento define cuánto tiempo puede utilizar la computadora la dirección IP asignada a ella antes de solicitar de nuevo una dirección desde el servidor DHCP. El parámetro de duración del arrendamiento depende del modo como trabajan los usuarios de la red. Si ésta es una pequeña red de una institución educativa, donde numerosos estudiantes llegan con sus computadoras portátiles para llevar a cabo pruebas, prácticas de laboratorio o talleres, la duración del arrendamiento puede ser el tiempo requerido para efectuar el trabajo. Si ésta es una red corporativa, donde los empleados trabajan tiempos regulares, el tiempo de arrendamiento podrá ser significativamente más extenso: varios días o semanas.

El servidor DHCP debe estar localizado dentro de la misma subred que los clientes, tomando en cuenta que éstos envían solicitudes de transmisión a él. Para reducir el riesgo de una falla de la red debido a mal funcionamiento del servidor DHCP, en ocasiones se instala un servidor DHCP redundante en la red. Esta variante corresponde a la configuración de la *red 1* mostrada en la figura 17.8.

En ocasiones existe un patrón opuesto: no hay servidores DHCP en la red. En este caso, el servidor DHCP es reemplazado por el agente de relevo DHCP (un software especializado que lleva a cabo el papel de mediador entre los clientes DHCP y los servidores DHCP). Un ejemplo de una configuración de este tipo se muestra mediante la *red 2* en la figura 17.8. El agente redirecciona las solicitudes del cliente desde la red local hasta uno de los servidores

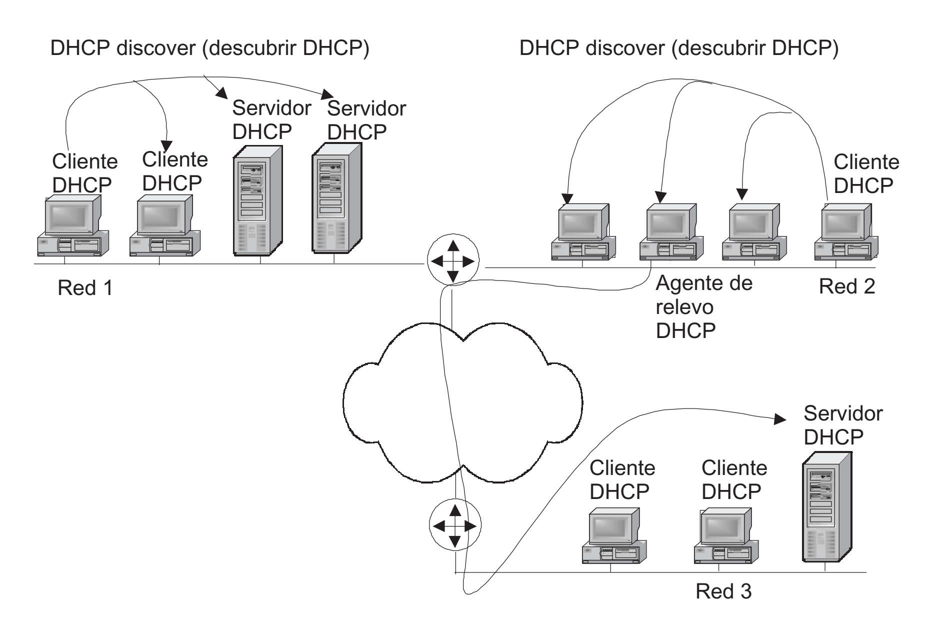


FIGURA 17.8 Métodos de disposición mutua de clientes y servidores DHCP.

DHCP localizado en otra subred (en dicho ejemplo, ésta es la *red 3*). Así, un servidor DHCP puede servir a los clientes DHCP de varias subredes.

El ejemplo siguiente es un método simplificado de intercambio de mensajes entre un cliente DHCP y el servidor.

Cuando una computadora se enciende, el cliente DHCP envía un mensaje de transmisión limitado conocido como *DHCPdiscover* (un paquete IP con una dirección de destino que incluye sólo unos binarios, el cual debe entregarse a todos los hosts dentro de esta red IP).

Los servidores DHCP localizados dentro de una red reciben este mensaje. Si la red no contiene servidores DHCP, el mensaje *DHCPdiscover* es recibido por el agente de relevo DHCP, el cual envía el mensaje a otra red, probablemente distante, hacia el servidor DHCP cuya dirección IP conoce de antemano.

Todos los servidores DHCP que han recibido el mensaje *DHCPdiscover* envían sus ofertas hacia el cliente DHCP que ha enviado solicitudes. Las ofertas se envían en mensajes *DHCPoffer,* cada uno de los cuales contiene una dirección IP y otra información de configuración (un servidor DHCP localizado en otra red envía su respuesta a través del agente).

El cliente DHCP recoleta las ofertas de configuración de todos los servidores DHCP. Como una regla, selecciona la primera oferta de los mensajes *DHCPoffer* que recibe y envía un mensaje de transmisión *DHCPrequest* que contiene información acerca del servidor DHCP cuya oferta ha sido aceptada (con los valores de los parámetros de configuración).

Todos los servidores DHCP reciben el mensaje *DHCPrequest* y el servidor DHCP seleccionado por el cliente envía el mensaje *DHCPacknowledgement* (confirmación de la dirección IP y parámetros de arrendamiento). Los otros servidores cancelan sus ofertas y regresan las direcciones ofrecidas a sus conjuntos de direcciones disponibles.

El cliente DHCP recibe la confirmación *DHCPacknowledgement* y entra en el estado de operación.

De tiempo en tiempo, la computadora intenta renovar los parámetros de arrendamiento obtenidos desde el servidor DHCP. Emprende el primer intento antes de que expire el término de arrendamiento y solicita al mismo servidor desde el que ha recibido a los parámetros

actuales. Si no hay respuesta o si ésta es negativa, repetirá su intento para enviar la solicitud después de algún tiempo. Si después de varios intentos repetidos el cliente falla en recibir los parámetros desde el mismo servidor, lo solicitará a otro servidor. Finalmente, si el intento de obtener parámetros desde otro servidor también falla, el cliente perderá sus parámetros de configuración y entrará en el modo de operación autónomo.

El cliente DHCP también puede liberar los parámetros en arrendamiento antes de lo programado si lleva a cabo el comando de liberación *DHCP*.

En una red en la que las direcciones IP se asignan de forma dinámica, no es posible decir cuál dirección se asigna a un host específico. Esta inconstancia de las direcciones IP produce algunos problemas. En primer lugar, *pueden surgir algunas dificultades cuando se traduce un nombre de dominio simbólico a una dirección IP.* ¡Imagine el lector la operación del DNS que debe soportar tablas de mapeo de nombres de dominio a direcciones IP cuando las últimas cambian cada dos horas! Con base en esta circunstancia, se recomienda asignar direcciones estáticas a los servidores en las que los usuarios suelen tener acceso por nombre simbólico y dejar sólo los nombres dinámicos para computadoras cliente. Sin embargo, en algunas redes, el número de servidores es tan grande que su configuración manual se convierte en una tarea demasiado intensiva. Esta situación dio lugar al diseño de una versión DNS mejorada, conocida como *DNS dinámica*, que se apoya en el uso coordinado de la base de datos de información de direcciones por los servicios DHCP y DNS.

En segundo lugar, *será bastante más difícil llevar a cabo el control remoto y monitoreo automático* (por ejemplo, para acumular estadísticas) para la interfase si se utiliza una dirección IP asignada de manera dinámica como su identificador.

Por último, para garantizar la seguridad de la red, la mayoría de los dispositivos de red pueden filtrar paquetes cuyos campos tengan valores predefinidos. En otras palabras, cuando se utilizan direcciones IP dinámicamente asignadas, *el filtrado de paquetes por direcciones IP se vuelve complicado.*

Los dos últimos problemas se resuelven con mayor facilidad al abandonar el uso de direcciones dinámicas para las interfases empleadas en sistemas de monitoreo y sistemas de seguridad.

RESUMEN

- La pila TCP/IP utiliza tres tipos de direcciones: direcciones locales (también conocidas como direcciones de hardware), direcciones IP y nombres simbólicos de dominio. Todos estos tipos de direcciones se asignan de manera independiente a los hosts de la interred.
- Una dirección IP tiene 4 bytes de longitud y consta del número de red y el número de host. Para determinar la frontera que separa el número de red del número de host, se utilizan dos enfoques: el primero está basado en clases de dirección, mientras que el segundo se apoya en el uso de máscaras.
- Una clase de dirección se define por los valores de varios bits de inicio de la dirección. En las direcciones clase A, 1 byte almacena un número de red y los 3 bytes restantes almacenan el número de host. La direcciones de clase A se utilizan en las redes más grandes. Para redes más pequeñas, las direcciones de clase C son las más adecuadas. En la direcciones de clase C, el número de red toma 3 bytes, mientras que para la numeración del host puede utilizarse 1 byte. Las redes de clase B se encuentran en una posición intermedia.

- Para separar una dirección IP en un número de red y número de host, se utiliza la máscara de red asociada con esta dirección. La representación binaria de la máscara contiene unos en aquellos bits que deben interpretarse como el número de red en la dirección IP actual.
- Las direcciones IP identifican unívocamente el host dentro de los límites de la interred; por lo tanto, deben asignarse de manera central.
- Si la red es pequeña y autónoma, la unicidad de las direcciones IP dentro de los límites de esta red puede asegurarse por medio del administrador de la red. El administrador es libre de elegir cualquier dirección IP para numeración de redes y hosts. El único requisito es que las direcciones seleccionadas deben tener la sintaxis correcta. No obstante, es preferible utilizar las denominadas direcciones privadas destinadas para las redes autónomas.
- Si una red es muy grande, como Internet, el proceso de asignación de direcciones IP será demasiado complicado y se dividirá en dos etapas. En la primera se distribuyen las direcciones de red. Esta etapa la regula una autoridad administrativa especial, que asegura la unicidad de la numeración de la red. Después de que la red recibe el número, tiene lugar la segunda etapa: la asignación de direcciones a sus hosts.
- La asignación de direcciones IP para los hosts de red puede llevarse a cabo de forma manual o de manera automática. Si las direcciones IP se asignan manualmente, el administrador de la red soportará las listas de direcciones de red tanto asignadas como disponibles y configurará de modo manual cada interfase de red. Cuando las direcciones IP se asignan de forma automática, se utiliza DHCP. En este caso, el administrador ha asignado con anterioridad un intervalo de direcciones disponibles al servidor DHCP y el servidor las asigna de manera automática a los hosts de red en respuesta a sus solicitudes.
- El establecimiento del mapeo entre una dirección IP y la dirección de hardware de la interfase de red se lleva a cabo mediante ARP.
- En redes con soporte de transmisión y en aquellas que no la soportan, se utilizan dos enfoques diferentes para resoluciones de dirección. Cuando ARP funciona en redes Ethernet, Token Ring y FDDI para traducir una dirección IP en una dirección MAC, se lleva a cabo una solicitud ARP de transmisión. Las respuestas ARP que llegan a la interfase se guardan en las tablas creadas en cada interfase de red. En redes que no soportan direcciones de transmisión, las tablas ARP se almacenan de forma central en el servidor ARP dedicado.
- La pila TCP/IP utiliza un sistema de dominio de nombres simbólicos, el cual tiene una estructura de árbol jerárquico que permite usar un número arbitrario de componentes en un nombre. Los nombres para los cuales coinciden los diversos componentes más significativos conforman el dominio del nombre. Los nombres de dominio se asignarán de manera central si la red es parte de Internet; de otro modo, se asignarán de forma local.
- La correspondencia entre los nombres de dominio y las direcciones IP puede establecerse mediante el uso de un archivo de host local y al emplear el servicio DNS centralizado fundamentado en la base de datos distribuida de los mapeos "nombre de dominio-dirección IP".

PREGUNTAS DE REPASO

1. ¿Cuál es la diferencia en los procedimientos para asignar direcciones de hardware y direcciones de red?
2. ¿Cuáles de las direcciones enumeradas aquí podrían utilizarse como direcciones locales en la intrarred IP? Y ¿cuáles direcciones no pueden emplearse de esta manera?
   a) Una dirección MAC de 6 bytes, como 12-B3-3B-51-A2-10.
   b) Una dirección X.25, como 25012112654987.
   c) Una dirección IPX de 12 bytes, como 13.34.B4.0A.C5.10.11.32.54.C5.3B.0.
   d) Una dirección VPI/VCI de una red ATM.
3. ¿Cuáles de estas afirmaciones son siempre correctas?
   a) Cada interfase de cada puente (bridge) o conmutador (switch) tiene una dirección MAC.
   b) Cada puente o conmutador tiene una dirección de red.
   c) Cada interfase del puente o conmutador tiene una dirección de red.
   d) Cada enrutador tiene una dirección de red.
   e) Cada interfase del enrutador siempre tiene una dirección MAC.
   f) Cada interfase de un enrutador tiene una dirección de red.
4. ¿Cuáles de las direcciones proporcionadas aquí no pueden utilizarse como direcciones IP de interfases de redes para hosts de Internet? Para las direcciones que no contengan errores de sintaxis, determine la clase: A, B, C, D o E.

a) 120.0.0.1	*e*) 10.234.17.25	*i*) 193.256.1.16
b) 201.13.123.245	*f*) 154.12.255.255	*j*) 194.87.45.0
c) 226.4.37.105	*g*) 13.13.13.13	*k*) 195.34.116.255
d) 103.24.254.0	*h*) 204.0.3.1	*l*) 161.23.45.305

5. Supóngase que una dirección IP de algún host de una subred es 198.65.12.67; el valor de máscara para esta subred es 255.255.255.240. Determine el número de subred. ¿Cuántos hosts puede contener esta subred?
6. Supóngase que usted conoce el mapeo entre las direcciones IP y los nombres de dominio para todas las computadoras en una red, excepto una. Para esa computadora, solamente se conoce el nombre del dominio. Con esta información, ¿puede usted definir su dirección IP con certidumbre?
7. ¿Cuántas tablas ARP existen en una computadora?, ¿cuántas hay en un enrutador? y ¿cuántas tiene un conmutador o switch?
8. De manera funcional, el ARP puede dividirse en la parte del cliente y la del servidor. Describa las funciones de las partes del cliente y del servidor.
9. ¿Cuáles son las direcciones que incluye un administrador en una tabla ARP?, ¿con qué propósito?
10. ¿En qué casos es útil emplear Proxy-ARP?
11. ¿Es posible determinar a partir de los nombres de dominio de las computadoras qué tan cerca se encuentran geográficamente entre sí?
12. Cierta computadora tiene la dirección IP 204.35.101.24 y el nombre de dominio new.firm.net. Determine cuál, si existe, de los siguientes nombres de dominio pertenece a otra computadora que tiene la dirección IP 204.35.101.25: new1.firm.net, new.firm1.net o new.1firm.net.
13. ¿Cuáles son las características comunes de DNS y el sistema de archivo?
14. ¿Cuántos servidores DHCP son suficientes para dar servicio a una red dividida por dos enrutadores?

15. Por confiabilidad, existen dos servidores DHCP en la red. ¿Cómo debería asignar el administrador el conjunto de direcciones disponibles para cada uno de ellos: asignar las partes que no se traslapan del conjunto a cada uno, o asignar el conjunto en común para ambos?
16. ¿Por qué un problema DNS inverso (encontrar nombres de host por medio de direcciones IP conocidas) no se resuelve sólo con usar el mismo enfoque que el empleado para resolver el problema directo (es decir, usual utilizar la misma zona y archivos de dominio organizados como un árbol correspondientes a la jerarquía de nombres)?

PROBLEMAS

1. Supóngase que algún ISP tiene una dirección de red de clase B a su disposición. Para los host de direccionamiento de su propia red, este ISP utiliza 254 direcciones. Determine el máximo número de clientes al que este ISP puede dar servicio si los tamaños de sus redes corresponden a la clase C. ¿Qué máscara debería establecerse en el enrutador del ISP que conecta su red con las redes de sus clientes?
2. ¿Cuál es el máximo número teórico de subredes que usted puede organizar si tiene una red de clase C a su disposición?, ¿cuál es el papel que desempeña una máscara de red en este caso? y ¿cuál es su valor?

18

PROTOCOLO DE INTERNET

DESCRIPCIÓN DEL CAPÍTULO

18.1 INTRODUCCIÓN

En este capítulo, la atención se centrará en el Protocolo de Internet (IP) definido en RFC 751. En cada red subsiguiente a lo largo de la trayectoria del paquete IP, este protocolo llama a las herramientas de transporte adoptadas en la red actual para utilizarlas en la entrega del paquete al ruteador conectado a la siguiente red o directamente al nodo de destino. De esta manera, una de las funciones IP más importantes es el soporte de la conexión a las tecnologías subyacentes de las redes constituyentes. Las funciones del IP incluyen conexión de soporte a los protocolos de las capas superior y de red y, en particular, a TCP, lo que en la pila TCP/IP lleva a cabo todas las tareas necesarias para asegurar la entrega confiable de datos mediante el uso de Internet.

IP es un protocolo sin conexión, lo cual significa que procesa cada paquete IP como una unidad independiente de datos que no tiene relación con otros paquetes IP. Además, IP no tiene mecanismos que suelen ponerse en marcha para asegurar la autenticidad de los datos que se entregan. Si se ha presentado algún error durante el envío del paquete, IP no inicia ninguna acción para corregirlo. Por ejemplo, si se descartó un paquete en uno de los ruteadores de tránsito debido al error de suma de verificación, la entidad IP no intenta retransmitir el paquete perdido. En otras palabras, IP implementa la política del mejor esfuerzo.

En este capítulo se verá con detalle la función principal de IP, el enrutamiento. Se explicará la estructura de las tablas de enrutamiento, tanto con máscaras como sin ellas; se darán ejemplos con el uso de máscaras de longitudes tanto física como variable, espacios de dirección con traslape y la aplicación de tecnologías de subred y superred y posteriormente se investigará la capacidad de IP para fragmentar paquetes.

Cuando se describan características específicas de IPv6, el interés se centrará en la modernización del método de direccionamiento, el cual permite contar con mejor escalabilidad. También se estudiará el formato del encabezado IP, que mejora el ancho de banda de la red al reducir la cantidad del trabajo delegado a los ruteadores.

18.2 FORMATO DE PAQUETE DE IP

PALABRAS CLAVE: protocolo de Internet, versión, IPv4, IPv6, paquete IP, tipo de servicio (ToS, Type Of Service), byte de servicios diferenciados (DS-byte, Differentiated Services Byte), precedencia de criterio de selección de ruta, Bandera (Flag), desplazamiento de fragmento (Offset Fragment), tiempo de vida (TTL, Time To Live), suma de verificación del encabezado (Header Checksum), dirección IP fuente, dirección IP destino, opciones de IP y relleno (padding).

Existe una relación directa entre el número de campos en el encabezado del paquete y la complejidad funcional del protocolo que trabaja con este encabezado. Cuanto más simple sea el encabezado, más simple resultará el protocolo correspondiente. La mayoría de las operaciones de protocolo se relacionan con el procesamiento de información de control conducida en los campos del encabezado del paquete. Al estudiar el valor de cada campo en el encabezado del paquete IP, no sólo se adquiere un conocimiento formal de la estructura del paquete, sino también se llegan a conocer las funciones principales del **Protocolo de Internet**.

El paquete IP incluye el encabezado y el campo de datos. El encabezado abarca los campos siguientes (figura 18.1):

Versión. Este campo toma 4 bits y especifica la versión IP. Actualmente, **IPv4** se utiliza casi en todas partes, pero la versión más reciente, **IPv6**, cada vez es más común.

Longitud de encabezado. El campo *Header Length* del paquete IP también tiene 4 bits y especifica la longitud del encabezado, medido en palabras de 32 bits. Por lo regular, el encabezado es de 20 bytes de longitud (cinco palabras de 32 bits). Sin embargo, si se agrega la información de control, esta longitud podrá incrementarse al utilizar bytes adicionales en el campo de opciones IP. La máxima longitud del encabezado es de 60 bytes.

Tipo de servicio (ToS), también conocido por su nuevo nombre: **byte de servicios diferenciados (DS-byte)**. Este campo tiene 1 byte. Dos variantes corresponden a los nombres de este campo: ToS (la interpretación principal) y DS-byte (el significado más reciente). En ambos casos, este campo se usa para almacenar parámetros que reflejan los requerimientos QoS del paquete.

En ToS, este campo se encuentra subdividido en dos subcampos. Los tres bits de inicio conforman el subcampo Precedence (de precedencia). La precedencia (es decir, la prioridad) puede tomar valores desde 0 (un paquete normal) hasta 7 (el paquete de información de control). Los ruteadores y computadoras pueden tomar en cuenta la prioridad del paquete y procesar los paquetes con la prioridad más alta en primer lugar. El campo *ToS* también contiene 3 bits que determinan el **criterio de selección de ruta**. Existen tres alternativas: retardo corto, alta confiabilidad o utilización elevada. Si el bit de *retardo* (D, *delay*) se establece con el valor de uno, se elegirá la ruta para minimizar el retardo en la entrega de este paquete. El bit de *utilización* (T, *throughput*) maximiza la utilización, mientras que el bit de *confiabilidad* (R, *reliability*) maximiza la confiabilidad. Los dos bits restantes están reservados y siempre establecidos en cero.

Los estándares de los servicios diferenciados adoptados hacia finales de la década de 1990 han dado un nuevo nombre a este campo y redefinido los valores de sus bits. DS-byte emplea sólo los seis bits más significativos de este byte y reserva los dos menos significativos. El propósito de cada bit del campo *DS-byte* se explicará en el capítulo 20 en la sección que describe los métodos para asegurar QoS en redes IP.

Longitud total. Este campo de 2 bytes caracteriza la longitud total del paquete, con base en el encabezado y el campo de datos. La longitud máxima del paquete se halla limitada por la longitud de este campo y el de 65 535 bytes. Sin embargo, la mayoría de la redes no utilizan paquetes tan extensos. Cuando se transmiten los paquetes a través de una red heterogénea, la longitud del paquete se elige con la cuenta de la longitud máxima del paquete del protocolo de capa inferior, que conduce los paquetes IP. Si éstos son tramas de Ethernet, la longitud máxima del paquete será de 1 500 bytes, debido a que un paquete así se ajustará dentro del

4 bits Número de versión	4 bits Longitud del encabezado	8 bits Tipo de servicio (ToS o DS-byte) PR | D | T | R	16 bits Longitud total
16 bits Identificación (ID de paquete)		3 bits Banderas D | M	13 bits Desplazamiento o compensación del fragmento
8 bits Tiempo de vida	8 bits Protocolo de capa superior	16 bits Suma verificadora del encabezado	
32 bits Dirección IP fuente o de origen			
32 bits Dirección IP de destino			
Parámetros y alineación			

FIGURA 18.1 Estructura del encabezado del paquete IP.

campo de datos de la trama de Ethernet. Los estándares TCP/IP toman provisiones para asegurar que todos los hosts sean capaces de recibir paquetes con una extensión de 576 bytes (sea que estén o no fragmentados).

Identificación. Este campo tiene 2 bytes y se emplea para identificar los paquetes creados como consecuencia de la fragmentación del paquete fuente. Todos los fragmentos del mismo paquete deben tener el mismo valor en este campo.

Banderas (flags). Las banderas poseen 3 bits y contienen atributos relacionados con la fragmentación. Al establecer con el valor de uno el bit de *no fragmentación* (DF, por sus siglas para *do not fragment*) se instruye al ruteador para que no fragmente este paquete. Si el bit de *más fragmentos* (MF, por las siglas para *more fragments*) se establece a uno, significará que dicho paquete está fragmentado y que no es el último. El bit restante está reservado.

Desplazamiento de fragmento (Fragment Offset). Este campo toma 13 bits y especifica el desplazamiento (en bytes) del campo de datos de este paquete desde el punto de inicio del campo de datos del paquete fragmentado fuente. Se utiliza cuando se ensamblan o reensamblan paquetes. El desplazamiento debe ser un múltiplo de 8.

Tiempo de vida (time to live). Este campo toma un byte y se utiliza para especificar el intervalo máximo de tiempo durante el cual el paquete puede viajar a través de la red. El TTL es medido en segundos y especificado por el remitente. El TTL actual del paquete es disminuido en uno cada segundo que gasta el paquete en cada ruteador a través del cual pasa durante su viaje a través de la red. Incluso si un ruteador procesa el paquete en menos de un segundo, todavía deberá disminuir el contador TTL en uno. Como los ruteadores contemporáneos raras veces toman más de un segundo para procesar un paquete, el TTL puede interpretarse como un número máximo de nodos de tránsito a través de los cuales puede pasar el paquete. Si el valor TTL alcanza el cero antes de entregarse el paquete al host de destino, el paquete se descartará. De este modo, el parámetro TTL es una especie de contador de "autodestrucción" para el paquete.

Protocolo. Este campo tiene un byte y contiene el identificador que especifica el protocolo de capa superior para el que está destinada la información en el campo de datos. Los valores del identificador para diversos protocolos se enumeran en los "números asignados" RFC. Hasta 1992 éstos eran RFC 1340; más adelante dicho RFC recibió el número 1700 (RFC 1700) y RFC 3232 fue renovado en 2002. En la actualidad, los RFC se encuentran disponibles en **http://www.iana.org**, el cual se actualiza con regularidad. Por ejemplo, el número 6 significa que el paquete contiene el mensaje TCP, 17 significa UDP y 1 indica ICMP.

Suma verificadora del encabezado. Este campo toma 2 bytes y se calcula únicamente para el encabezado. Como algunos campos del encabezado cambian valores en el curso de la transmisión del paquete a través de la red (por ejemplo, TTL), la zona verificadora tiene que revisarse y volver a calcularse en cada enrutador y en cada nodo. La suma de verificación (16 bits) es calculada como complemento a la suma de todas las palabras de 16 bits del encabezado. Cuando se calcula la suma verificadora, el valor del campo (*Header Checksum*, *suma verificadora del encabezado*) se establece a cero. Si el valor de la suma de verificación es incorrecto, se informará del error y se descartará el paquete en el mismo instante en que se detecte ese error.

Dirección IP fuente y dirección IP destino. Estos campos tienen la misma longitud: 32 bits.

Opciones de IP. Este campo es opcional. Como regla, se utiliza solamente cuando se efectúa la detección de problemas en la red. Este campo contiene varios subcampos, cada uno compuesto de ocho tipos predefinidos. En dichos subcampos, es posible especificar la ruta exacta para el paso por los enrutadores, registrar los enrutadores recorridos por el paquete, almacenar los datos del sistema de seguridad o guardar marcas de tiempo.

Relleno. Como el número de subcampos en los campos de *Opciones de IP* (*IP Options*) pueden ser arbitrarios, es necesario agregar varios bytes al final del encabezado del paquete para alinear dicho paquete con la frontera de 32 bits. Los campos de relleno se llenan con ceros.

A continuación se muestra el listado de los campos de encabezado de un paquete real de IP capturado de Ethernet al usar el analizador de protocolo Monitor de Red (NM, por las siglas en inglés para Network Monitor). En este listado, NM proporciona valores hexadecimales de los campos (entre paréntesis); además, el programa reemplaza en ocasiones los códigos numéricos de los campos con información por un formato más amigable con el usuario. Por ejemplo, la interfase NM reemplaza el código en el campo *Protocol* (*Protocolo*) con un nombre de protocolo (en este caso, reemplaza el código 6 con la cadena de caracteres TCP: véase la línea en negritas, a continuación).

```
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: Total Length = 54 (0x36)
IP: Identification = 31746 (0x7C02)
IP: Flags Summary = 2 (0x2)
IP: .......0 = Last fragment in datagram
IP: ......1. = Cannot fragment datagram
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = TCP — Transmission Control
IP: Checksum = 0xEB86
IP: Source Address = 194.85.135.75
IP: Destination Address = 194.85.135.66
IP: Data: Number of data bytes remaining = 34 (0x0022)
```

18.3 MÉTODO DE ENRUTAMIENTO DE IP

PALABRAS CLAVE: enrutamiento, tabla de enrutamiento para ruta, dirección de destino del paquete, interfase, puerto, distancia, clase de servicio, ruta específica, ruta predeterminada, compuerta, salto siguiente, tabla de enrutamiento mínima, red conectada directamente, dirección de paso inverso, protocolo de enrutamiento, servidor/cliente DNS, respuesta DNS, consulta DNS, diagrama de datos UDP y servidor/cliente FTP.

Considérese el método de enrutamiento IP en el ejemplo de la interred que muestra la figura 18.2. Esta red comprende 20 enrutadores (designados por los cuadrados numerados) que unen 18 redes en una interred: N1, N2,..., N18 que representan los números de red. IP se instala en cada enrutador y en los nodos terminales A y B.

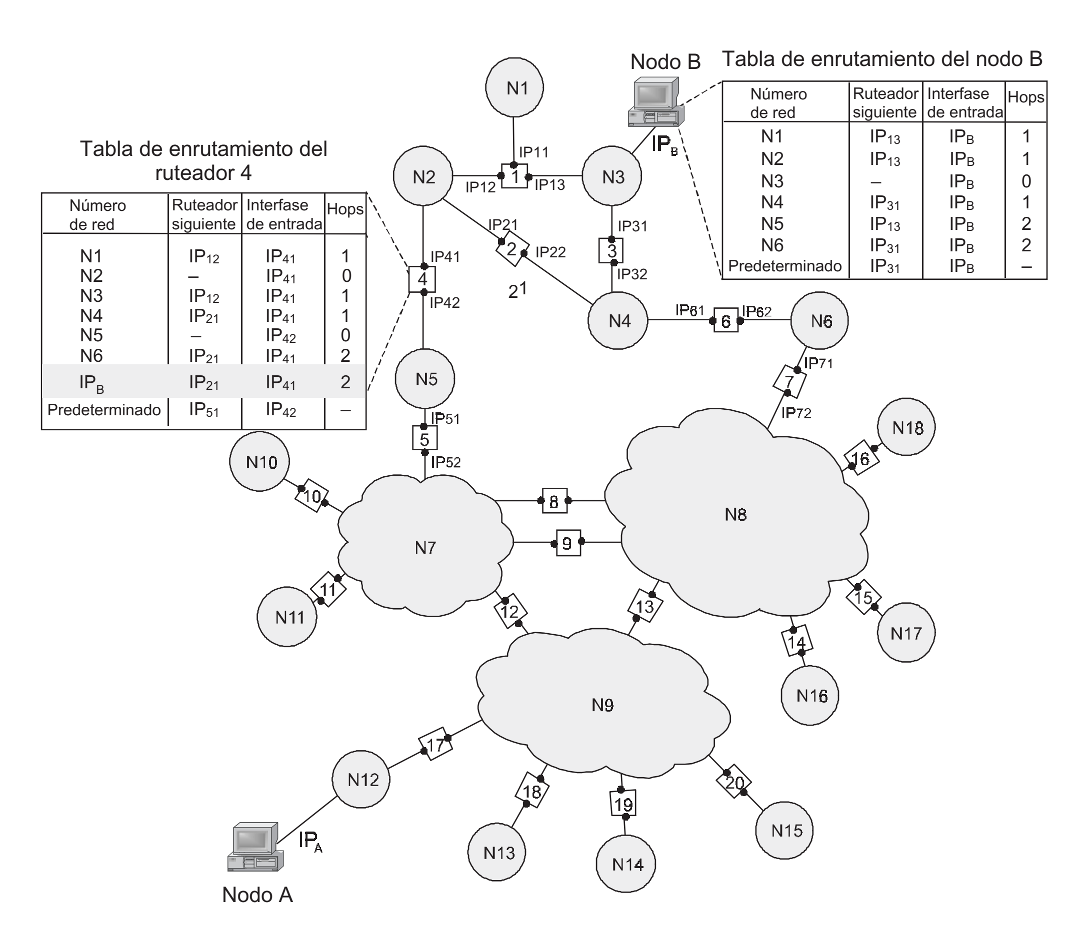


FIGURA 18.2 Principios de enrutamiento en interredes.

Los ruteadores tienen varias interfases (puertos) a las que se conectan las redes. Cada interfase de ruteador puede considerarse un nodo de red individual: tiene una dirección de red por separado y la dirección local de la red conectada a él. Por ejemplo, el ruteador 1 tiene tres interfases a las que están conectadas las redes N1, N2 y N3. En la ilustración, las direcciones de red de estos puertos se clasifican como IP_{11}, IP_{12} e IP_{13}. La interfase IP_{11} es el nodo de la red N1; en consecuencia, el campo del número de red de la dirección IP^{11} contiene el número N1. De manera similar, la dirección IP_{12} es el nodo de la red N2 y la dirección IP_{13} representa el nodo de la red N3. Así, se puede estimar que un ruteador es un conjunto de nodos, cada uno de los cuales forma parte de una red individual. Como dispositivo unificado, el ruteador no tiene una red ni una dirección local.

NOTA *Si un ruteador posee una unidad de control (por ejemplo, una unidad de control SNMP), tiene sus propias direcciones local y de red, por medio de las cuales se puede tener acceso a él a través de la estación de control central.*

En intrarredes complejas, siempre hay varias rutas para transmisión de paquetes entre dos nodos terminales. Por ejemplo, el paquete enviado desde el nodo A hasta el nodo B puede pasar a través de los ruteadores 17, 12, 5, 4 y 1 o a través de los ruteadores 17, 13, 7, 6 y 3. No es difícil encontrar otras rutas entre los nodos A y B.

El problema de seleccionar el ruteador es resuelto por los ruteadores y los nodos terminales. El ruteador se elige con base en la información de la configuración actual de la red

proporcionada a aquellos dispositivos y según el criterio de selección de la ruta. Con bastante frecuencia, el retardo del paso de un paquete individual a lo largo de la ruta, el ancho de banda promedio de la ruta para la secuencia del paquete o incluso el criterio más simple basado sólo en el número de ruteadores de tránsito que pasan a lo largo de la ruta (hops) son criterios de selección de ruta. Toda la información acerca de las rutas que se obtiene como resultado de este análisis se coloca en la **tabla de enrutamiento**.

18.3.1 Estructura simplificada de la tabla de enrutamiento

Se utilizará notación convencional para el diseño de las direcciones de red de los números de red y ruteadores en la forma mostrada en la figura 18.2. Con esta notación, considérese el aspecto que tendría la tabla de enrutamiento de, digamos, el ruteador 4 (tabla 18.1).

NOTA *La tabla 18.1 está considerablemente simplificada en comparación con las tablas de enrutamiento reales. Por ejemplo, esta tabla no proporciona los campos que contienen valores de máscara. También carece de campos que contienen indicadores del estado de ruta y valores TTL de los registros de la tabla. El uso de estos atributos se verá más adelante. En lugar del número de red de destino, puede especificarse un nodo de destino de dirección de red completamente calificada. Aparte de esto, como ya se mencionó, esta tabla proporciona direcciones de red en un formato convencional. Esto significa que, en el presente ejemplo, las direcciones de red no corresponden a un protocolo de red en específico. No obstante, esta tabla contiene los campos principales presentes en las tablas de enrutamiento reales.*

El primer campo de esta tabla contiene las **direcciones de destino del paquete**.

En cada fila de la tabla 18.1, la dirección de destino es seguida de la **dirección de red del ruteador siguiente**. Para ser más precisos, ésta es la dirección de red de la interfase correspondiente del siguiente ruteador al cual debe enviarse el paquete para dirigirse hacia la dirección de destino a lo largo de una ruta racional.

Antes de pasar el paquete al ruteador siguiente, el ruteador actual debe detectar a cuál de sus puertos (IP_{41} o IP_{42}) debe enviarse este paquete. Para tal propósito, se utiliza el tercer

TABLA 18.1 Tabla de enrutamiento del ruteador 4

Dirección de destino	Dirección de red del ruteador siguiente	Dirección de red del puerto de salida	Distancia desde la red de destino (hops)
N1	IP_{12} (R1)	IP_{41}	1
N2	–	IP_{41}	0 (conectada)
N3	IP_{12} (R1)	IP_{41}	1
N4	IP_{21} (R2)	IP_{41}	1
N5	–	IP_{42}	0 (conectada)
N6	IP_{21} (R2)	IP_{21}	2
IP_B	IP_{21} (R2)	IP_{41}	2
Predeterminada	IP_{51} (R5)	IP_{42}	–

campo de la tabla de enrutamiento, el cual contiene las **direcciones de red de las interfases de salida**.

Algunas implementaciones de los protocolos de red toleran la existencia de varias filas correspondientes a la misma dirección de destino en la tabla de enrutamiento. En este caso, cuando se elige la ruta, se toma en cuenta la **distancia desde el campo de red de destino**. La distancia se interpreta como cualquier métrica utilizada de acuerdo con el criterio especificado en el paquete de red (este criterio se denomina a menudo **clase de servicio**). La distancia puede medirse como el número de hops, el tiempo requerido por el paquete para pasar a través de enlaces de comunicaciones o una característica de confiabilidad de enlace específico en la ruta elegida. También puede representarse por cualquier otro valor que refleje la calidad de esta ruta en relación con el criterio especificado. En la tabla 18.1, la distancia entre redes se midió en hops. Para redes directamente conectadas a los puertos de ruteador, se supone que la distancia es 0, aunque algunas implementaciones comienzan el conteo de las distancias desde 1.

Cuando el paquete llega al ruteador, la entidad IP recupera el número de red de destino del encabezado de la trama entregada y lo compara de forma secuencial con los números de red de cada fila de la tabla de enrutamiento. La fila con el número coincidente indica cuál es el ruteador más próximo hacia el que es necesario enviar el paquete. Por ejemplo, si un paquete destinado a la red N6 llega a cualquier puerto del ruteador 4, la tabla de enrutamiento mostrará que la dirección del siguiente ruteador es IP_{21}. Esto significa que en la siguiente etapa del proceso de envío, dicho paquete se enviará hacia el puerto 1 del ruteador 2.

Con mucha frecuencia, las tablas de enrutamiento especifican los números de red de destino en lugar de las direcciones IP completas. De este modo, para todos los paquetes enviados hacia la misma red, IP sugerirá la misma ruta (por el momento, no se toman en cuenta los posibles cambios en el estado de la red, como fallas del ruteador o rupturas de cable). Sin embargo, en algunos casos, se debe seleccionar una **ruta específica** para uno de los nodos de la red, ruta que difiere de la especificada para los otros nodos de la red. Para conseguir esto, es necesario introducir una fila por separado para este host en la tabla de enrutamiento, fila que debe contener la dirección IP completa del host junto con la información apropiada de la ruta. Un registro de dicha clase para el host B se aprecia en la tabla 18.1. Por ejemplo, supóngase que el administrador del ruteador 4, con base en consideraciones de seguridad, decide que todos los paquetes destinados al host B (la dirección IP completa es IP_B) deben pasar a través del ruteador 2 (la interfase IP_{21}) en lugar de hacerlo a través del ruteador 1 (la interfase IP_{12}), a través del cual los paquetes se pasan a los otros hosts de la red N3. Si la tabla contiene registros que especifican rutas tanto hacia la red completa como hacia uno de sus hosts, el ruteador dará preferencia a la ruta específica cuando el paquete destinado a este host llegue al ruteador.

Como el paquete puede estar destinado a cualquier subred de la interred, puede parecer que cada tabla de enrutamiento debería contener los registros de *todas* las redes incluidas en la red. Sin embargo, en redes grandes este enfoque es ineficaz debido a que las tablas de enrutamiento crecen de manera significativa. La búsqueda en una gran tabla de enrutamiento requiere mucho tiempo; además, una tabla así necesita más espacio de almacenamiento. Por consiguiente, en la práctica, es mejor reducir el número de registros en la tabla de enrutamiento mediante el uso de un registro especial conocido como **ruta predeterminada**. Si se considera la topología de la interred, se descubrirá que las tablas de enrutamiento de los ruteadores localizados en la periferia de la interred pueden registrar sólo los números de las redes directamente conectadas a ellos o localizadas cerca de las rutas terminales. Al igual que con otras redes, es suficiente incluir el registro único en la tabla de enrutamiento y especificar la trayectoria hasta el ruteador a través de la cual pasa la trayectoria hacia estas

redes. Un ruteador de esta naturaleza se conoce como **ruteador predeterminado**. En lugar del número de red, la fila apropiada de la tabla de enrutamiento debe contener un registro específico que se llama **predeterminado**. En nuestro ejemplo, el ruteador 4 especifica las trayectorias únicamente para los paquetes que viajan hacia las redes N1-N6. Para los otros paquetes destinados a las redes N7-N18, este ruteador sugiere el mismo puerto, IP_{51} del mismo ruteador, el 5.

18.3.2 Tablas de enrutamiento en nodos terminales

El problema del enrutamiento se resuelve no sólo con nodos de tránsito (ruteadores) sino también mediante nodos terminales (computadoras). El proceso para resolver este problema comienza cuando el IP instalado en el nodo terminal detecta si se envía el paquete a otra red o si se dirige a un host específico dentro de los límites de esta red. Si el número de la red de destino coincide con el de esta red, no deberá mandarse tal paquete; de otra manera, será necesario el enrutamiento.

Las estructuras de las tablas de enrutamiento de nodo terminal y nodo de tránsito son similares. Una vez más, considérese la red que aparece en la figura 18.2. La tabla de enrutamiento del nodo terminal B perteneciente a la red N3 puede tener el aspecto de la mostrada en la tabla 18.2. Aquí, IP_B es la interfase de red de la computadora B. Con base en esta tabla, la computadora B elige a cuál de los dos ruteadores en la red local N3 (R1 o R3) debería enviar paquetes específicos.

Los nodos terminales utilizan la técnica de enrutamiento predeterminada incluso a mayor escala que los ruteadores. Aunque en general también tienen tablas de enrutamiento a su disposición, el volumen de tales tablas suele ser pequeño, lo cual se debe a que se localizan nodos terminales en la periferia de la red. Con bastante frecuencia, los nodos terminales funcionan sin tablas de enrutamiento. En tales casos, utilizan solamente la información acerca de la dirección del ruteador predeterminado. Esta variante es la única posible para todos los nodos terminales si sólo se encuentra un ruteador en la red constituyente. Sin embargo, incluso si existen varios ruteadores en la red constituyente y el nodo terminal tiene que elegir el correcto, suele especificarse la ruta predeterminada para mejorar el rendimiento de la computadora.

TABLA 18.2 Tabla de enrutamiento de la computadora B

Número de la red de destino	Dirección de la red del ruteador siguiente	Dirección de la red del puerto de salida	Distancia hacia la red de destino
N1	IP_{13} (R1)	IP_B	1
N2	IP_{13} (R1)	IP_B	1
N3	–	IP_B	0
N4	IP_{31} (R3)	IP_B	1
N5	IP_{13} (R1)	IP_B	2
N6	IP_{31} (R3)	IP_B	2
Predeterminada	IP_{31} (R3)	IP_B	–

TABLA 18.3 Tabla de enrutamiento del nodo terminal A

Número de la red de destino	Dirección de la red del ruteador siguiente	Dirección de la red del puerto de salida	Distancia hacia la red de destino
N12	–	IP_A	0
Predeterminada	$IP_{17,1}$ (R17)	IP_A	–

La tabla 18.3 muestra la tabla de enrutamiento de otro nodo terminal de la interred: el host A. El pequeño tamaño de esta tabla de enrutamiento refleja que todos los paquetes enviados desde el nodo A deben pasar a través del puerto 1 del ruteador 17 o no dejar nunca los límites de la red N12. Tal ruteador se define como el ruteador predeterminado en esta tabla de enrutamiento.

Otra diferencia entre el comportamiento de un ruteador y el de un nodo terminal es el método para elaborar la tabla de enrutamiento. Como regla, los ruteadores crean la tabla de enrutamiento de manera automática mediante el intercambio de información de control. En contraste, las tablas de enrutamiento para los nodos terminales se crean a menudo de forma manual por los administradores, en cuyo caso se guardan en discos fijos como archivos normales.

18.3.3 Tablas de rutina de búsqueda que no contienen máscaras

El algoritmo de consulta de la tabla de enrutamiento utilizado por el IP instalado en el ruteador se describe en esta sección. Cuando se explique este algoritmo, se usarán la tabla 18.1 y la figura 18.2.

- Supóngase que un paquete llega a uno de los puertos del ruteador. El IP recupera la dirección IP de destino del paquete recién llegado. Por claridad, supóngase también que este paquete especifica IP_B en el campo de dirección de destino.
- Se lleva a cabo la *primera fase* de la consulta de tabla: consiste en *la búsqueda de una ruta específica hacia el host de destino*. IP_B se compara de manera secuencial, fila por fila, con el contenido del campo de **dirección de destino** de la tabla de enrutamiento. Si hay una coincidencia (como en el ejemplo con la tabla 18.1), se recuperará la dirección del siguiente ruteador (IP_{21}) desde la fila apropiada junto con el identificador de la interfase de salida (IP_{41}). El procedimiento de consulta de la tabla se consigue en esta etapa.
- Ahora supóngase que la tabla no contiene una fila con la dirección de destino IP_B, lo cual significa que no se encontró ninguna coincidencia. En este caso, IP procede con la *segunda fase* de la consulta de tabla. La segunda fase de este proceso consiste en *la búsqueda de la ruta hacia la red de destino*. El número de red se recupera desde la dirección IP (en este ejemplo, la red N3 se recuperará desde la dirección IP_B) y se repite la consulta de tabla. Esta vez, es necesario hallar un número de red que coincida con el número de red especificado en el paquete. Si se encuentra una coincidencia (como en el ejemplo), se recuperará la dirección del siguiente ruteador (IP_{12}) y el identificador de la interfase de salida (IP_{41}) desde la fila apropiada de la tabla. Cuando se lleva a cabo esta operación, se ha realizado la consulta de tabla.
- Finalmente, supóngase que ni la primera ni la segunda fases de la consulta de la tabla de enrutamiento producen una coincidencia para la dirección de destino en el paquete reci-

bido. En este caso, el IP elige la ruta predeterminada, en cuyo caso el paquete parte hacia la dirección IP_{51}, o descartará el paquete si no hay una ruta predeterminada. Entonces, se ha llevado a cabo la consulta de tabla.

IMPORTANTE *Aquí, el punto principal es que la secuencia de las fases de consulta de tabla se encuentra definida de manera estricta, pero el orden de las filas en la tabla de enrutamiento, incluida la posición del registro que especifica a la ruta predeterminada no influye en el resultado.*

18.3.4 Ejemplos de tablas de enrutamiento de diferentes formatos

La estructura de las tablas de enrutamiento reales de la pila TCP/IP por lo general corresponde a la estructura simplificada de las tablas de enrutamiento consideradas con anterioridad. Sin embargo, el formato de la tabla de enrutamiento IP específica depende de la instalación de la pila TCP/IP. Considérense diversas versiones de las tablas de enrutamiento con las cuales funciona el ruteador R1 en la red mostrada en la figura 18.3.

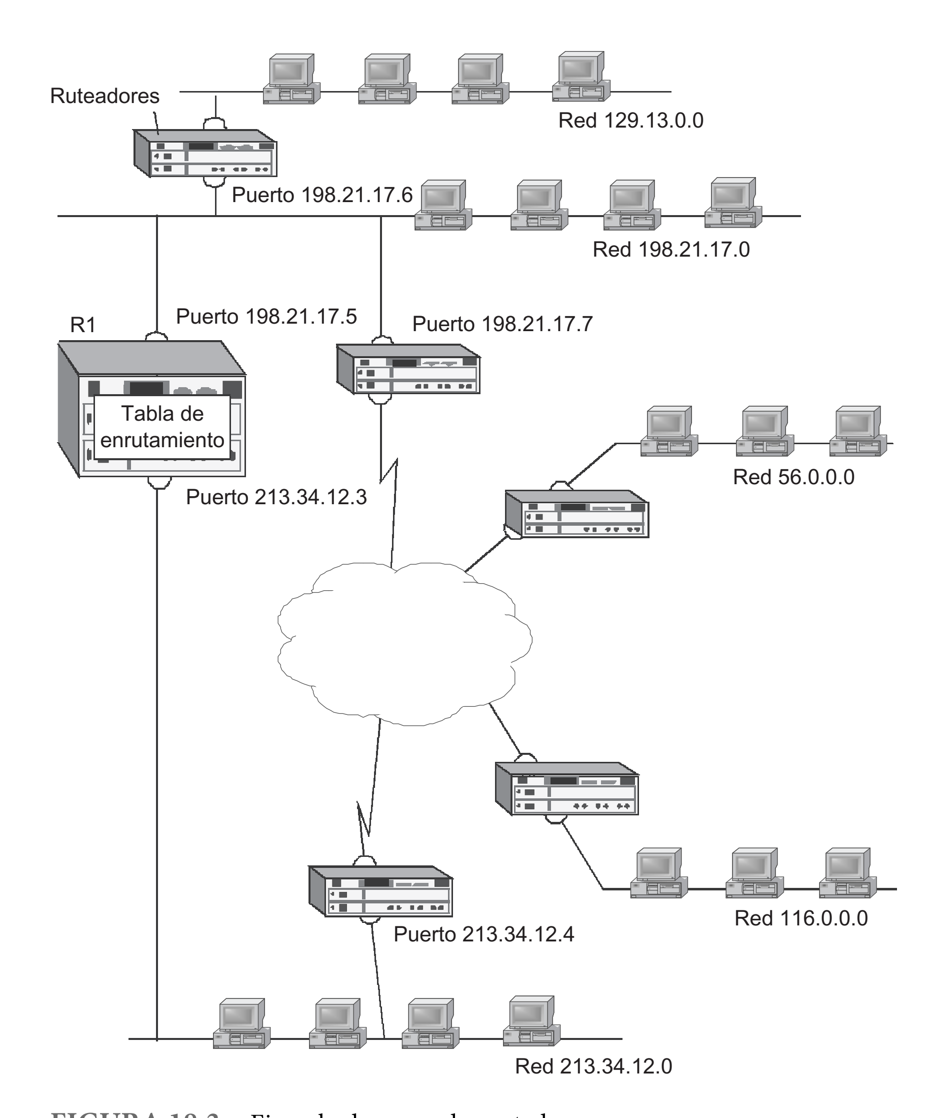


FIGURA 18.3 Ejemplo de una red enrutada.

Comience con una variante algo artificial y simplista de la tabla de enrutamiento (tabla 18.4). Aquí, existen rutas hacia las redes (registros 56.0.0.0, 116.0.0.0 y 129.13.0.0), dos registros en las redes conectadas directamente (129.13.0.0 y 213.34.12.0) y un registro en la ruta predeterminada.

Las tablas de enrutamiento generadas en equipo de red fabricado industrialmente tienen un formato más complejo.

TABLA 18.4 Tabla de enrutamiento simplificada del ruteador R1

Dirección de la red de destino	Dirección de la red del ruteador siguiente	Dirección de la interfase de salida	Distancia hacia la red de destino
56.0.0.0	213.34.12.4	213.34.12.3	15
116.0.0.0	213.34.12.4	213.34.12.3	13
129.13.0.0	198.21.17.6	198.21.17.5	2
129.13.0.0	198.21.17.5	198.21.17.5	1
213.34.12.0	213.34.12.3	213.34.12.3	1
Predeterminada	198.21.17.7	198.21.17.5	–

TABLA 18.5 Tabla de enrutamiento del ruteador integrado de Windows 2000

Dirección de la red	Máscara de la red	Dirección de la compuerta	Interfase	Métrica
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.5	1
56.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	15
116.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	13
129.13.0.0	255.255.0.0	198.21.17.6	198.21.17.5	2
198.21.17.0	255.255.255.0	198.21.17.5	198.21.17.5	1
198.21.17.5	255.255.255.255	127.0.0.1	127.0.0.1	1
198.21.17.255	255.255.255.255	198.21.17.5	198.21.17.5	1
213.34.12.0	255.255.255.0	213.34.12.3	213.34.12.3	1
213.34.12.3	255.255.255.255	127.0.0.1	127.0.0.1	1
213.34.12.255	255.255.255.255	213.34.12.3	213.34.12.3	1
224.0.0.0	224.0.0.0	198.21.17.6	198.21.17.6	1
224.0.0.0	224.0.0.0	213.34.12.3	213.34.12.3	1
255.255.255.255	255.255.255.255	198.21.17.6	198.21.17.6	1

Si se supone que el ruteador R1 en la red actual es el ruteador de software construido en el sistema operativo Microsoft Windows 2000, su tabla de enrutamiento tendrá un aspecto parecido al que aparece en la tabla 18.5.

Si se reemplaza el ruteador R1 con uno de los de hardware conocidos, la tabla de enrutamiento para la misma red tendrá un aspecto diferente, por ejemplo, como el que se muestra en la tabla 18.6.

Por último, la tabla 18.7 representa una tabla de enrutamiento para el mismo ruteador R1 implementado en forma de ruteadores de software de uno de los sistemas operativos de la familia UNIX.

NOTA *Como no existe correspondencia no ambigua entre la estructura de la red y la tabla de enrutamiento, es posible sugerir versiones específicas para cada variante suministrada de la tabla de enrutamiento. Estas versiones pueden diferir en la ruta elegida a la red específica, en cuyo caso se debe poner atención a las diferencias significativas en la forma de representar la información de enrutamiento al usar diferentes implementaciones de ruteadores.*

A pesar de las notorias diferencias, los datos clave requeridos por IP para el enrutamiento del paquete se encuentran en las tres tablas de enrutamiento reales.

TABLA 18.6 Tabla de enrutamiento de un ruteador de hardware

Destino	Máscara	Compuerta	Métrica	Estado	TTL	Fuente u origen
198.21.17.0	225.255.255.0	198.21.17.5	0	Up	_	Conectado
213.34.12.0	225.255.255.0	213.34.12.3	0	Up	_	Conectado
56.0.0.0	225.0.0.0	213.34.12.4	14	Up	_	Estático
116.0.0.0	225.0.0.0	213.34.12.4	12	Up	_	Estático
129.13.0.0	225.255.0.0	198.21.17.6	1	Up	160	RIP

TABLA 18.7 Tabla de enrutamiento del ruteador UNIX

Destino	Compuerta	Banderas	Refcnt	Uso	Interfase
127.0.0.0	127.0.0.1	UH	1	154	lo0
Predeterminado	198.21.17.7	UG	5	43270	le0
198.21.17.0	198.21.17.5	U	35	246876	le0
213.34.12.0	213.34.12.3	U	44	132435	le1
129.13.0.0	198.21.17.6	UG	6	16450	le0
56.0.0.0	213.34.12.4	UG	12	5764	le1
116.0.0.0	213.34.12.4	UG	21	23544	le1

La lista de tales datos incluye **direcciones de la red de destino** (los campos de *destino* en el ruteador de hardware y el ruteador UNIX, así como el campo de *dirección de red* en el ruteador de Windows 2000). Otro campo requerido de la tabla de enrutamiento es la dirección del siguiente ruteador (los campos de *compuerta* o *gateway* en el ruteador de hardware y en el de UNIX, así como el campo de *dirección de compuerta* en el de Windows 2000).

El tercer parámetro clave es la **dirección del puerto hacia el cual debería enviarse el paquete**. En algunas tablas de enrutamiento se especifica directamente (el campo de *interfase* en el ruteador de Windows 2000), mientras que en otras tablas se especifica de manera implícita. Por ejemplo, la tabla de enrutamiento del ruteador UNIX señala el nombrado convencional del puerto en lugar de su dirección: *le0* para el puerto con la dirección 198.21.17.5, *le1* para el puerto con la dirección 213.34.12.3 y *lo0* para el puerto interno con la dirección 127.0.0.1.

En el ruteador de hardware, falta el campo que especifica el puerto de salida en cualquier forma, lo cual se debe a que la dirección del puerto de salida siempre puede definirse indirectamente por la dirección del siguiente ruteador. Por ejemplo, intente determinar la dirección del puerto de salida para la red 56.0.0.0 con base en la tabla 18.6, la cual revela que el siguiente ruteador para esta red será el ruteador con la dirección 213.34.12.4. La dirección del siguiente ruteador debe pertenecer a una de las redes conectadas directamente a este ruteador, en cuyo caso la red es la 213.34.12.0. El ruteador tiene el puerto conectado a esa red. La dirección de este puerto, 213.34.12.3, puede encontrarse en el campo de *compuerta* de la segunda fila de la tabla de enrutamiento, que describe la red de 213.34.12.0 conectada directamente. Para redes conectadas en forma directa, la dirección del enrutador siguiente siempre es la dirección del puerto de salida del enrutador local. De este modo, para la red 56.0.0.0, la dirección del puerto de salida será 213.34.12.3.

En la actualidad, el uso del campo de máscara en cada registro de la tabla de enrutamiento es una solución estándar. Considérese, por ejemplo, la tabla de enrutamiento del ruteador de Windows 2000 (el campo *máscara de red*) y la del ruteador de hardware (el campo *máscara*). El procesamiento de la máscara en los ruteadores cuando se decide cuál será el enrutamiento del paquete se considerará más adelante en este capítulo. La ausencia del campo de máscara especifica que el ruteador está proyectado para funcionar sólo con las tres clases de dirección estándar o que utiliza la misma máscara para todos los registros, lo cual reduce la flexibilidad del enrutamiento.

Como cada red de destino se menciona solamente una vez en la tabla de enrutamiento del ruteador de UNIX, no hay elección para seleccionar la ruta. Por lo tanto, en este caso la métrica es un parámetro opcional. En otras tablas se halla presente este campo; no obstante, se utiliza sólo como indicador de la red conectada en forma directa. En consecuencia, la métrica 0 para el ruteador de hardware o de 1 para el ruteador de Windows 2000 simplemente informa al ruteador que esta red se encuentra conectada de manera directa a su puerto. Otros valores de la métrica corresponden a redes remotas. La elección del valor de la métrica para la red conectada directamente (1 o 0) es arbitraria. El punto principal aquí es que la métrica de la red remota debe contarse con este valor inicial seleccionado.

> *El indicador de la red conectada directamente* informa al ruteador que el paquete ha llegado a su red de destino. Por ende, el ruteador no lo pasa al siguiente ruteador. En cambio, el paquete pasa directamente hacia el host de destino, de modo que IP inicia una solicitud ARP acerca de la dirección IP del host de destino en lugar de la correspondiente al siguiente ruteador.

Sin embargo, a veces el ruteador debe almacenar el valor de la métrica para el registro de cada red remota. Tales situaciones surgen cuando los registros en la tabla de enrutamiento

son resultado de la operación de varios protocolos de enrutamiento, como RIP. En dichos protocolos, la información recién recibida de cualquier red remota se compara con información en la tabla. Si el nuevo valor de la métrica es mejor que el actual, un nuevo registro reemplazará al existente. En la tabla del ruteador UNIX, el campo de métrica está ausente, lo cual significa que este ruteador no utiliza RIP.

Las banderas se encuentran presentes sólo en la tabla del ruteador UNIX y describen las siguientes características del registro:

- *U*: especifica que la ruta está activa y es utilizable. El campo de *estado* de la tabla de enrutamiento del ruteador de hardware tiene un significado similar.
- *H*: indica la ruta específica a cierto host.
- *G*: señala que la ruta del paquete pasa a través del ruteador de tránsito (compuerta). Si no existe esta bandera, la red se hallará conectada de manera local.
- *D*: especifica que la ruta se ha obtenido del mensaje de *redirección* (*redirect*) de ICMP. Esta bandera puede presentarse solamente en la tabla de enrutamiento del nodo terminal. Si está activa, significa que el nodo terminal en uno de los intentos anteriores para transmitir el paquete seleccionó el ruteador siguiente, que no fue el óptimo. Este ruteador, en el cual se usa ICMP, ha informado que los paquetes futuros destinados a esta red deben enviarse a través de otro ruteador.

En las tablas de enrutamiento de los ruteadores UNIX existen otros dos campos que contienen valores de referencia. El campo *refcnt* especifica cuántas veces se hizo referencia a esta ruta en el curso del envío del paquete, mientras que el campo *use* indica el número de bytes enviados a lo largo de esta ruta.

Las tablas de enrutamiento de los ruteadores de hardware también tienen dos campos de referencia. En este caso, el campo de *tiempo de vida* (TTL) no tiene relación con el tiempo de vida del paquete. Como en muchas otras tablas, dicho campo evita usar registros cuyo contenido puede ser obsoleto. El valor actual del campo *TTL* especifica el TTL del registro, es decir, el intervalo de tiempo (en segundos) durante el cual este registro permanecerá válido. El campo *fuente* (*source*) especifica la fuente desde la cual este registro ha aparecido en la tabla de enrutamiento. Aunque dicho campo no está presente en todos los ruteadores, existen tres fuentes principales de registros para prácticamente todos los ruteadores.

18.3.5 Fuentes y tipos de registros en tabla de enrutamiento

Para casi todos los ruteadores existen *tres* fuentes principales de registros:

- Una de las fuentes de registros en la tabla de enrutamiento es *el software que implementa la pila TCP/IP*. Cuando se inicializa un ruteador, este software inserta de manera automática varios registros en la tabla de enrutamiento. Como resultado, se crea la **tabla de enrutamiento mínima**.

  La lista de tales registros incluye información acerca de **redes conectadas directamente** y **rutas predeterminadas** que por lo regular se introducen cuando se configuran en forma manual las interfases de una computadora o un ruteador. En los ejemplos dados, los registros en las redes son 213.34.12.0 y 198.21.17.0, el registro de la ruta predeterminada en el ruteador UNIX, así como el registro 0.0.0.0 en el ruteador de Windows 2000.
- El software TCP/IP también introduce información de manera automática acerca de direcciones especiales en la tabla de enrutamiento. En los ejemplos proporcionados, la tabla de enrutamiento para el ruteador de Windows 2000 contiene el conjunto más completo

de tales registros. Varios registros en esta tabla se relacionan con la **dirección de anillo** (127.0.0.0) utilizada para la prueba local de la pila TCP/IP. Los registros con la dirección de destino 224.0.0.0 son necesarios para procesar direcciones multicast. Aparte de ello, la tabla puede contener direcciones destinadas para transmisiones de procesamiento (por ejemplo, los registros 8 y 11 contienen la dirección del mensaje de transmisión en las subredes apropiadas y el último registro de esta tabla contiene la dirección de transmisión limitada). Nótese que los registros para direcciones especiales deben estar ausentes de algunas tablas de enrutamiento.

- La segunda fuente de registros en la tabla de enrutamiento es la *entrada manual*. Un administrador de red forma directamente tales registros con alguna utilidad de red especializada, como el programa route suministrado con UNIX y Windows 2000. En los ruteadores de hardware también existe un comando especial para crear registros de forma manual en la tabla de enrutamiento. Los registros elaborados así siempre son estáticos, lo cual significa que no tienen término de expiración. Estos registros pueden ser persistentes (es decir, se mantienen después de reinicializar el ruteador) o temporales (o sea, se almacenan en la tabla de enrutamiento sólo hasta que es apagado el dispositivo). A menudo los administradores diseñan de forma manual el registro en la ruta predeterminada, y los registros en rutas específicas para ciertos hosts pueden crearse de la misma manera.
- Finalmente, los *protocolos de enrutamiento* como RIP u OSPF pueden ser la tercera fuente de registros en la tabla de enrutamiento. Estos registros siempre son dinámicos, lo cual significa que tienen una TTL limitada.

Los ruteadores de software construidos en los sistemas operativos Windows 2000 y UNIX exhiben la fuente desde la que ha aparecido el registro específico en la tabla de enrutamiento. Por el contrario, un ruteador de hardware utiliza el campo *source* o *fuente* para este propósito. En el ejemplo de la tabla 18.6, los primeros registros se hicieron mediante el software de pila TCP/IP con base en los datos de configuración del puerto. Esto lo muestra el atributo *connected*. Los dos registros siguientes se designan como *static* o *estáticos*, lo cual quiere decir que el administrador los introdujo de forma manual. El último registro apareció como resultado de la operación RIP; por consiguiente, su campo *TTL* contiene el valor 160.

18.3.6 Ejemplo de enrutamiento IP sin máscaras

Considérese el proceso de envío del paquete sobre la interred en el ejemplo de la red IP ilustrada en la figura 18.4. En este ejemplo, suponga que todos los hosts de la red tienen direcciones basadas en clases. Debería ponerse interés especial a la interacción de IP con ARP y DNS.

Supóngase que el usuario de la computadora llamada **cit.mgu.com**, localizada en la red Ethernet1 necesita establecer una conexión con el servidor FTP. El usuario conoce el nombre simbólico del servidor: **unix.mgu.com**. Por lo tanto, ese usuario emite el siguiente comando para tener acceso al servidor FTP por nombre:

```
> ftp unix.mgu.com
```

La ejecución de este comando puede representarse mediante un proceso de tres etapas:

- Pasar la consulta DNS desde el siguiente para determinar la dirección IP del host de destino.
- Pasar la respuesta DNS desde el servidor.

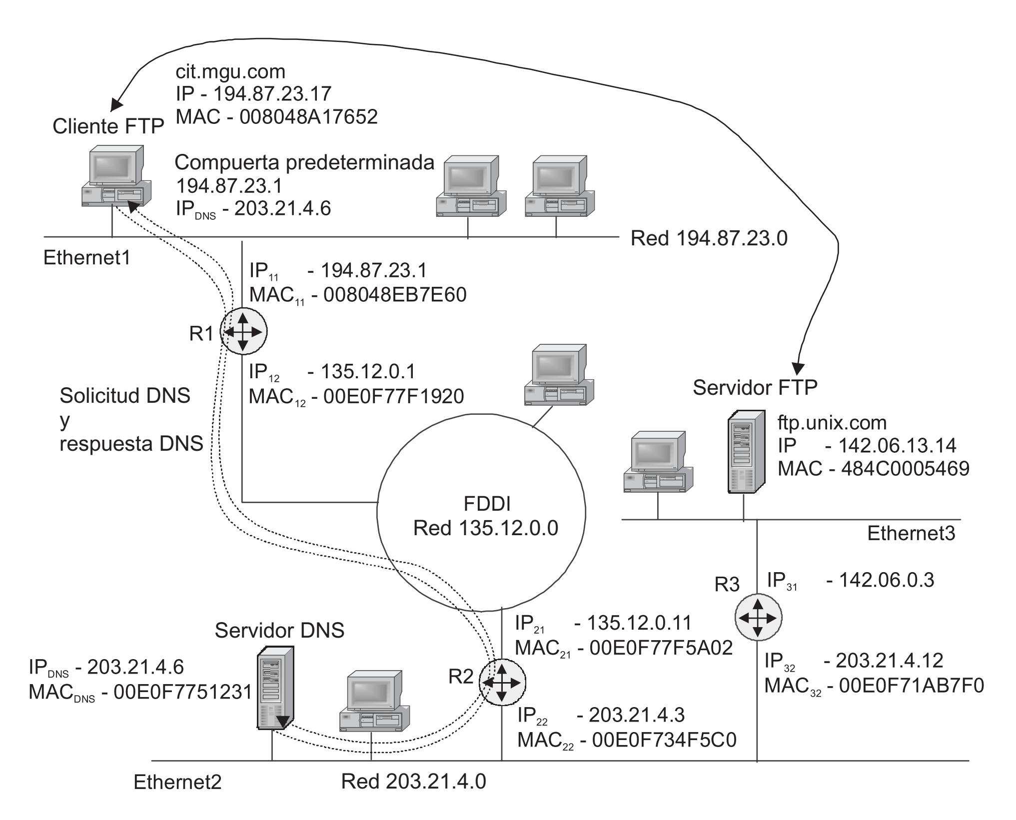


FIGURA 18.4 Ejemplo de enrutamiento IP.

- Transmitir del paquete desde el siguiente FTP hacia el servidor FTP.

  Así, comencemos desde la primera etapa.

Pasar una consulta DNS

1. El cliente FTP pasa la solicitud a la parte cliente del protocolo DNS que se ejecuta en la misma computadora. Este módulo, a su vez, formula la solicitud al servidor DNS. En su forma más general, dicha solicitud aparece como sigue: "¿cuál dirección IP corresponde al nombre simbólico **unix.mgu.com**?" La solicitud formulada es encapsulada en el datagrama UDP y luego dentro del paquete IP (figura 18.5). La dirección IP del servidor DNS (203.21.4.6) se especifica como la dirección de destino en el encabezado de este paquete. Tal dirección se conoce por el software cliente de la computadora, pues éste se especificó como un parámetro de configuración.
2. Antes de encapsular el mencionado paquete IP en la trama Ethernet, se debe averiguar si éste tiene que dirigirse a través de la interred o si está destinado para el host localizado

Encabezado IP		Encabezado UDP	Solicitud DNS
Dirección IP del emisor	Dirección IP del receptor		
194.87.23.17	203.21.4.6		

FIGURA 18.5 Paquete IP que contiene la solicitud DNS.

en la misma red como el remitente. Para tal propósito, IP compara los números de red en las direcciones fuente y destino, por ejemplo: 194.87.23.17 y 203.21.4.6. Como resultado de esta comparación, llega a ser evidente que el paquete está dirigido hacia otra red; en consecuencia, debe pasarse al ruteador más cercano. Como Ethernet1 contiene sólo un ruteador, R1, todos los nodos terminales de esta red utilizan la dirección de este ruteador (194.87.23.1) como predeterminado. Esta dirección también está especificada como un parámetro de configuración de la computadora cliente.

3. Con el fin de habilitar la red Ethernet1 para entregar el paquete al ruteador R1, debe colocarse este paquete en el campo de datos de la trama Ethernet y se le debe suministrar una dirección MAC. El problema se resolverá si se utiliza ARP, el cual busca la tabla ARP. Si la dirección requerida está ausente de la tabla, el host cliente enviará una solicitud ARP de transmisión: "¿Cuál dirección MAC corresponde a la dirección IP 194.87.23.1?" Todos los nodos de la red Ethernet1 reciben esta solicitud; sin embargo, únicamente la interfase 1 del ruteador R1 responde con la respuesta siguiente: "yo tengo la dirección IP 194.87.23.1 y mi dirección MAC es 008048EB7E60". Después de recibir esta información, el host **cit.mgu.com** envía el paquete IP a través de la red local. Este paquete es encapsulado en la trama Ethernet y tiene los campos mostrados en la figura 18.6.
4. La trama es recibida por la interfase 1 del ruteador R1. El protocolo Ethernet recupera el paquete IP de esta trama y lo pasa a IP, el cual recupera la dirección de destino, 203.21.4.6, de este paquete y busca en su tabla de enrutamiento local. Supóngase que el ruteador R1 tiene el registro siguiente en su tabla de enrutamiento:

   203.21.4.0   135.12.0.11 135.12.0.1

   Este registro especifica que los paquetes dirigidos a la red 203.21.4.0 deben pasarse al ruteador 135.12.0.11, localizado en la red conectada a la interfase 135.12.0.1 del ruteador R1. Dicho ruteador busca los parámetros de la interfase 135.12.0.1 y detecta que una red FDDI se encuentra conectada a ella. Como la red FDDI tiene un valor MTU más grande que la red Ethernet, no necesita fragmentarse el paquete IP. (Recuérdese que MTU es la máxima longitud del datagrama que puede caber en el campo de datos de la unidad de transmisión de una tecnología de red específica. La fragmentación se verá con mayor detalle más adelante en este capítulo.) Por consiguiente, el ruteador R1 forma una trama del formato FDDI.
5. En la etapa mencionada, la entidad IP del ruteador R1 debe determinar la dirección MAC del ruteador siguiente por su dirección IP conocida: 135.12.0.11. Para conseguir esto, depende de ARP. Supongamos que esta vez el siguiente registro estaba presente en la tabla ARP:

   135.12.0.11 -—   00E0F77F5A02

   Ahora, una vez conocida la dirección MAC del ruteador R2 (00E0F77F5A02), el ruteador R1 envía la trama (figura 18.7) a la red FDDI.

Encabezado Ethernet		Encabezado IP		Encabezado UDP	Solicitud DNS
Dirección MAC del emisor	Dirección MAC del receptor	Dirección IP del emisor	Dirección IP del receptor		
MACc-008048A17652	MAC_{11}-008048EB7E60	194.87.23.17	203.21.4.6		unix.mgu.com?

FIGURA 18.6 Trama Ethernet que contiene la solicitud DNS enviada desde la computadora cliente.

Encabezado FDDI		Encabezado IP		Encabezado UDP	Solicitud DNS
Dirección MAC del emisor	Dirección MAC del receptor	Dirección IP del emisor	Dirección IP del receptor		
MAC_{12}-00E0F77F1920	MAC_{21}-00E0F77F5A02	194.87.23.17	203.21.4.6		unix.mgu.com?

FIGURA 18.7 Trama FDDI que contiene la solicitud DNS enviada desde el ruteador R1 hacia el ruteador R2.

Encabezado Ethernet		Encabezado IP		Encabezado UDP	Solicitud DNS
Dirección MAC del emisor	Dirección MAC del receptor	Dirección IP del emisor	Dirección IP del receptor		
MAC_{21}-00E0F734F5C0	MAC_{DNS}-00E0F7751231	194.87.23.17	203.21.4.6		unix.mgu.com?

FIGURA 18.8 Trama Ethernet que contiene la solicitud DNS enviada desde el ruteador R2.

6. La entidad de IP que se ejecuta en el ruteador R2 continúa de manera semejante. Una vez recibida la trama FDDI, elimina su encabezado y recupera la dirección IP de destino del encabezado IP. Después de esto, busca en su tabla de enrutamiento, donde averigua que la red de destino está conectada directamente a su segunda interfase. Por lo tanto, envía la siguiente solicitud ARP a la red Ethernet2: "¿Cuál dirección MAC corresponde a la dirección IP 203.21.4.6?" Cuando recibe la respuesta en la dirección MAC del servidor DNS, 00E0F7751231, el ruteador R2 envía la trama mostrada en la figura 18.8 hacia la red Ethernet2.
7. El adaptador de red del servidor DNS captura la trama Ethernet, detecta que la dirección MAC de destino especificada en el encabezado coincide con su propia dirección MAC y la envía a su propia entidad IP. Después de analizar los campos del encabezado IP, el IP recupera los datos de los protocolos de capa superior del paquete. La consulta DNS se pasa entonces al módulo de software del servidor DNS, el cual busca en sus tablas, y posiblemente solicita otros servidores DNS. Como resultado de esta operación, formula la respuesta, que es como sigue: "El nombre simbólico unix.mgu.com tiene la dirección IP correspondiente 142.06.13.14".

NOTA *Durante todo el tiempo que el paquete viaja a través de la interred desde la computadora cliente hasta el servidor DNS, las direcciones fuente y de destino en los campos del encabezado IP nunca cambian. Sin embargo, las direcciones de hardware en los campos del encabezado de cada nueva trama que conduce el paquete entre un ruteador y otro cambian en cada sección de la trayectoria.*

Pasar una respuesta DNS

1. La pila TCP/IP instalada en el servidor DNS encapsula la respuesta DNS en el datagrama UDP, que se encapsula entonces en el paquete IP. Adviértase que la dirección IP de destino se conoce a partir de la consulta DNS. Posteriormente IP determina que tiene que dirigirse el paquete.

Encabezado Ethernet		Encabezado IP		Encabezado UDP	Solicitud DNS
Dirección MAC del emisor	Dirección MAC del receptor	Dirección IP del emisor	Dirección IP del receptor		
MAC_{11}-008048EB7E60	MACc-008048A17652	203.21.4.6	194.87.23.17		*142.06.13.14*

FIGURA 18.9 Trama Ethernet con la respuesta DNS enviada desde el ruteador R2.

2. IP busca la tabla de enrutamiento y determina la dirección IP del siguiente ruteador (IP22) 203.21.4.3.
3. ARP determina la dirección MAC de la interfase del ruteador: 00E0F734F5C0.
4. El paquete IP es colocado en el campo de datos de la trama Ethernet y enviado hacia la red Ethernet2.
5. El ruteador R2 recibe la trama y lleva a cabo las operaciones descritas en los pasos 2 y 3, luego de lo cual envía la trama FDDI al ruteador R1.
6. El ruteador R1 determina de la tabla de enrutamiento que el paquete que llega está destinado a la red directamente conectada a su interfase. Por lo tanto, IP solicita a ARP recibir la dirección MAC del nodo de destino en lugar de la del ruteador.
7. La trama (figura 18.9) destinada al cliente FTP se envía hacia la red Ethernet1.
8. El cliente FTP recibe la trama y recupera la respuesta que inicie de ahí. Ahora puede continuar la ejecución del comando, pues el nombre simbólico del servidor FTP se ha traducido a la forma de una dirección IP.

```
> ftp 142.06.13.14
```

Pasar el paquete desde un cliente FTP a un servidor FTP

Esta etapa es similar a los procedimientos descritos para trasmitir consultas respuesta que se inicien a través de la red. No obstante, escribir este proceso por sus propios medios será un ejercicio útil. Cuando realice esta tarea, el lector pondrá especial atención en los valores de los campos de la dirección de las tramas y los paquetes IP encapsulados.

18.4 ENRUTAMIENTO MEDIANTE EL USO DE MÁSCARAS

PALABRAS CLAVE: subred, ruteador, distribución del espacio de dirección, máscara, red no estructurada, división de una red, algoritmo para búsqueda en las tablas de enrutamiento, direcciones de destino recuperadas, zonas desmilitarizadas, prefijo, agregación de dirección, elaboración de subredes, elaboración de superredes ("superneteo"), enrutamiento de interdominio sin clase (CIDR, Classless InterDomain Routing), localización de dirección y espacios de dirección con traslape.

El algoritmo de enrutamiento es más complicado cuando elementos adicionales, las máscaras, se introducen en el sistema de direccionamiento del nodo. ¿Por qué se abandonó el método de direccionamiento basado en clases después de que había servido como una tecnología probada y eficaz durante años? La razón principal es la necesidad de estructurar la red cuando existe una escasez de números de red disponibles para distribución.

A menudo, los administradores de red se molestan porque la cantidad de números de red que se les asignan centralmente es insuficiente para estructurar de manera adecuada la

red. Por ejemplo, en una interred estructurada de manera adecuada, las computadoras que no interactúan de forma intensa y frecuente deben colocarse en redes diferentes. Existen dos maneras posibles de superar una situación así. El primer método implica obtener números de red adicionales de alguna autoridad centralizada; el segundo y más común se relaciona con el uso de la tecnología de máscaras, el cual permite dividir una red en varias subredes.

18.4.1 Estructura de una red con máscaras de la misma longitud

Por ejemplo, supóngase que un administrador ha obtenido una dirección de clase B: 129.44.0.0. Él puede organizar una gran red en la cual los números de host pueden asignarse desde el intervalo siguiente: 0.0.0.1-0.0.255.254. El número total de direcciones es 2^{16}, pues las direcciones conformadas únicamente con ceros o unos tienen significados especiales y no son convenientes para direccionamiento de host. Sin embargo, ese administrador no necesita una red no estructurada simple. Las necesidades de su compañía dictan otra solución. De acuerdo con esta solución, la red de la compañía debe dividirse en tres subredes por separado, de tal manera que el tráfico de cada subred se localiza de modo confiable. Una solución de esta naturaleza permitirá simplificar los diagnósticos y mantener la red. También ayudará a hacer cumplir la política de seguridad específica para cada subred. Otra ventaja importante de dividir una red grande mediante máscaras es que facilita que la estructura interna de la red de la compañía se encuentre oculta de observadores externos, lo cual mejora su seguridad.

La figura 18.10 muestra la división del espacio de dirección obtenido por el administrador de la red en cuatro partes iguales, cada una con 2^{14} direcciones. Como el número de bits requeridos para numerar los hosts ha disminuido en 2 bits, el prefijo de cada una de

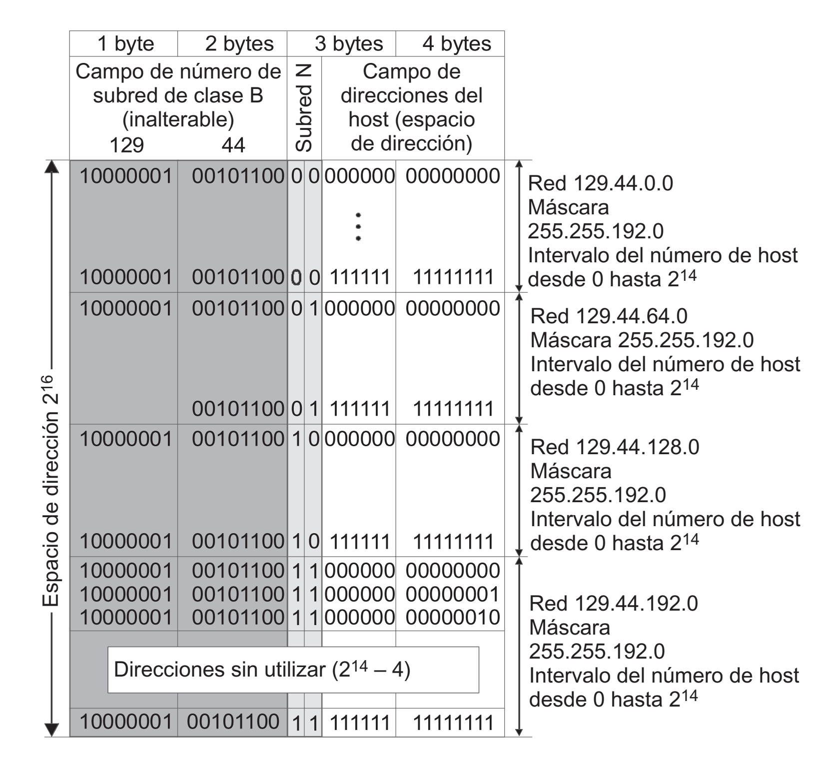


FIGURA 18.10 División del espacio de dirección de la red de clase B (129.44.0.0) en cuatro partes iguales.

las cuatro redes se hace 2 bits *mayor;* en consecuencia, cada intervalo de dirección puede escribirse en la forma de una dirección IP con una máscara que incluya 18 unos binarios o como 255.255.192.0 en notación decimal:

```
129.44.0.0/18        (10000001 00101100 00000000 00000000)
129.44.64.0/18       (10000001 00101100 01000000 00000000)
129.44.128.0/18      (10000001 00101100 10000000 00000000)
129.44.192.0/18      (10000001 00101100 11000000 00000000)
```

De los registros proporcionados con anterioridad, es claro que el administrador puede utilizar dos bits adicionales para numerar subredes. Esto le permite crear cuatro subredes del gran espacio de dirección que se le asignó de manera central. En este ejemplo, las subredes son: 129.44.0.0/18, 129.44.64.0/18, 129.44.128.0/18 y 129.44.192.0/18.

NOTA *Algunos ruteadores de software y hardware, que siguen recomendaciones obsoletas de [RFC 950], no soportan números de subredes que incluyan sólo unos o ceros. Para esta clase de equipo, el número de red 129.44.0.0 con la máscara 255.255.192.0, empleado en este ejemplo, será inválido, pues los bits en el número de subred tienen el valor de 00. De acuerdo con consideraciones semejantes, el número de red 129.44.192.0 con la misma máscara también será inválido. Aquí, el número de red abarca únicamente unos. No obstante, los ruteadores contemporáneos que soportan [RFC 1878] están libres de estas limitaciones.*

El ejemplo de una red creada al dividir una red grande en cuatro subredes de tamaño igual se muestra en la figura 18.11. Todo el tráfico que llega a la red interna 129.44.0.0 desde el exterior llega a través del ruteador R1. Para flujos de información de estructura adicionales, se encuentra instalado un ruteador adicional, R2, en la red interna. Todas las redes recién creadas, 129.44.0.0/18, 129.44.64.0/18, 129.44.128.0/18 y 129.44.192.0/18, se conectaron a puertos del ruteador interno R2 configurados de manera apropiada.

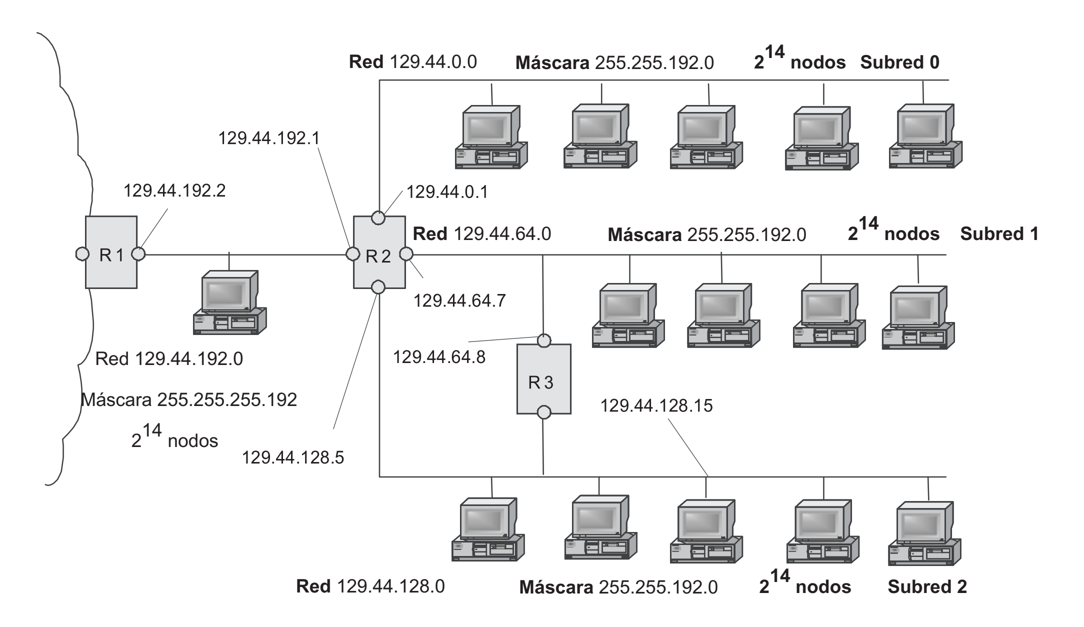


FIGURA 18.11 Enrutamiento en el que se usan máscaras de la misma longitud.

TABLA 18.8 Tabla de enrutamiento del ruteador R2 en la red con máscaras de la misma longitud

Dirección de destino	Máscara	Dirección del siguiente ruteador	Dirección del puerto	Distancia
129.44.0.0	255.255.192.0	129.44.0.1	129.44.192.2	Conectado
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Conectado
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Conectado
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Conectado
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–
129.44.128.15	255.255.255.255	129.44.64.8	129.44.64.7	–

NOTA *En una de esas redes, 129.44.192.0/18, dedicada a crear una conexión entre ruteadores externos e internos, únicamente se usaron dos direcciones: 129.44.192.1 (el puerto del ruteador R2) y 129.44.192.2 (el puerto del ruteador R1). Dos direcciones más, 129.44.192.0 y 129.44.192.255, tienen propósitos especiales. No se utilizan muchas direcciones en esta red (2^{14} – 4). Como es evidente, este ejemplo se ha seleccionado sólo para propósitos de demostración destinados a ilustrar la ineficacia de dividir la red en subredes de igual tamaño.*

Desde el exterior, esta red todavía parece una sola red de clase B. Sin embargo, todo el tráfico entrante en esta red está dividido por el ruteador local R2 entre cuatro subredes. Cuando el mecanismo de clase no funciona, el ruteador debe tener otro mecanismo que le permita detectar qué parte del número de 32 bits colocado en el campo de dirección de destino representa el número de red. Un campo de máscara adicional incluido en la tabla de enrutamiento (tabla 18.8) sigue este propósito.

Los primeros cuatro registros en esta tabla corresponden a las subredes internas conectadas en forma directa a los puertos del ruteador R2.

El registro 0.0.0.0 con la máscara 0.0.0.0 corresponde a la ruta predeterminada.

El último registro señala una ruta específica al host 129.44.128.15. Para los registros de la tabla que indican la dirección IP completa de una host, la máscara tiene el valor 255.255.255.255. En contraste con los otros nodos de la red 129.44.128.0, a la cual llegan los paquetes desde la interfase 129.44.128.5 del ruteador R2, para este host, los paquetes llegarán a través del ruteador R3.

18.4.2 Algoritmo para búsqueda en tabla que explica las máscaras

El algoritmo para búsqueda de las tablas de enrutamiento que contienen máscaras tiene mucho en común con el algoritmo descrito para las tablas que no contienen máscaras. No obstante, también contiene modificaciones significativas, a saber:

1. El IP comienza la búsqueda del ruteador siguiente para un paquete recién llegado al *recuperar la dirección de destino del paquete*. Para distinguirlo, la designaremos como IP_D. Después IP comienza procedimiento de búsqueda de la tabla de enrutamiento, el

cual de manera similar al de búsqueda de la tabla que no contiene el campo de máscara, también abarca dos fases.

2. La *primera fase consiste en la búsqueda de una ruta específica para la dirección* IP_D. Para conseguir esto, IP recupera la dirección de destino de cada registro de la tabla para que el valor de la máscara se encuentre establecido a 255.255.255.255. Las direcciones de destino recuperadas se comparan con la dirección de destino del paquete IP_D. Si se encuentra una coincidencia en cualquier registro, la dirección del ruteador siguiente se tomará de este registro.
3. La *segunda fase* se llevará a cabo si se ha buscado en toda la tabla pero no se ha encontrado una coincidencia completa de direcciones. Esta fase consiste en la búsqueda de una ruta no específica común para el grupo de hosts con los que se relaciona el paquete con la dirección IP_D. Para lograr esto, IP busca una vez más en la tabla de enrutamiento.
4. Las acciones siguientes se llevan a cabo para cada *registro siguiente*:
   - La máscara (M) contenida en el registro actual se "aplica" a la dirección IP del nodo de destino recuperado desde el paquete: IP_D AND M.
   - El resultado se compara con el valor colocado en el campo de dirección de destino del mismo registro de la tabla de enrutamiento.
   - Si se encuentra una coincidencia, IP *marcará este registro de manera apropiada.*
   - Si no se han rastreado todos los registros, IP procesará el registro siguiente (regrese al paso 4). Si se han procesado todos los registros, incluido el que contiene información acerca de la ruta predeterminada, el protocolo continuará con el paso 5.
5. Después de examinar toda la tabla de enrutamiento, el ruteador lleva a cabo una de las acciones siguientes:
   - Si no se ha encontrado una coincidencia y no existe ruta predeterminada, se descartará el paquete.
   - Si se ha hallado una coincidencia, el paquete se dirigirá a lo largo de la ruta especificada por el registro que contenga la dirección coincidente.
   - Si hay varias coincidencias, el protocolo comparará todos los registros marcados y elegirá la ruta especificada por registro con el número máximo de bits coincidentes. En otras palabras, cuando la dirección de destino indicada en el paquete pertenece a varias subredes, *el ruteador utiliza la ruta más específica.*

NOTA *En muchas tablas de enrutamiento, el registro con la dirección 0.0.0.0 corresponde a la ruta predeterminada. Cualquier dirección en el paquete entrante, después de aplicar la máscara 0.0.0.0, producirá la dirección de red 0.0.0.0, que corresponde a la dirección especificada en el registro. Como la máscara 0.0.0.0 tiene longitud cero, se considerará que esta ruta es la menos específica y se empleará únicamente si no hay coincidencias con otros registros de la tabla de enrutamiento.*

A continuación se ilustra cómo el ruteador R2 (figura 18.11) utiliza el algoritmo descrito para trabajar con su tabla de enrutamiento (tabla 18.8). Supóngase que un paquete con la dirección de destino *129.44.78.200* llega al ruteador R2. La entidad IP en ese ruteador comparará primero esta dirección con la dirección 129.44.128.15, para la que se ha definido una ruta específica. Como no hay coincidencia, IP procesará secuencialmente todas las filas de la tabla, de tal forma que aplicará las máscaras y comparará los resultados hasta que encuentre la coincidencia para el número de red tanto en la dirección de destino como en la fila de la tabla. De este modo, se ha encontrado la ruta para este paquete: debe enviarse

hacia el puerto del ruteador de salida 129.44.64.7 y hacia la red 129.44.64.0 conectada en forma directa a este ruteador.

18.4.3 Uso de máscaras de longitud variable

En muchos casos, es más eficaz dividir la red en subredes de diferentes tamaños. En particular, para la subred que conecta dos ruteadores de acuerdo con el método "punto a punto", incluso el número de direcciones disponibles en la red de clase C es demasiado grande.

La figura 18.12 muestra otro ejemplo de distribución del mismo espacio de dirección utilizado en el anterior ejemplo: 129.44.0.0/16. La mitad de las direcciones disponibles (2^{15}) están asignadas para crear una red con la dirección 129.44.0.0 y la máscara 255.255.128.0. El siguiente intervalo de direcciones, un cuarto del espacio de dirección completo (2^{14}), se asignó a la red 129.44.128.0 con la máscara 255.255.192.0.

Después de ello, se "cortó" un fragmento pequeño del espacio de dirección, destinado a crear una red para conectar el ruteador interno R2 al ruteador externo R1. Para numerar los hosts en una red degenerada de esta clase, es suficiente con asignar 2 bits. De cuatro posibles combinaciones de números de host (00, 01, 10 y 11), dos números tienen significado especial y no se pueden asignar a los hosts. Sin embargo, los dos números restantes, 10 y 01, son suficientes para direccionar los puertos del ruteador. En este caso, el campo de número de host tiene una longitud de 2 bits y la máscara en notación decimal aparecerá del modo siguiente: 255.255.255.252. El número de red, como se muestra en la figura 18.12, es 129.44.192.0.

NOTA *No es necesario asignar direcciones IP a enlaces punto a punto entre ruteadores, pues no pueden conectarse hosts a tales redes, excepto dos puertos del ruteador. No obstante, en la mayoría de los casos, los administradores eligen asignar una dirección IP para una red así. Por ejemplo, esto se hace para ocultar la estructura interna de la red y para tener acceso a la red mediante la dirección del puerto del ruteador de entrada con la aplicación de la técnica de traducción de dirección de red (NAT, Network Address Translation). En el presente caso, ésta es la dirección 129.44.192.1; además, tal dirección puede ser necesaria para "hacer un túnel" ("tuneleo") en el tráfico utilizando la red IP. Por ejemplo, este enfoque puede emplearse para "tunelear" el tráfico IPX o el tráfico IPSec encriptado. El "tuneleo" (tunneling) y NAT se examinarán en el capítulo 20.*

El espacio de dirección restante puede "seccionarse" en un número de redes de cualquier tamaño, según las necesidades de la compañía. Por ejemplo, un administrador puede crear una red bastante grande que contenga 2^{13} hosts del conjunto de direcciones restante (2^{14} – 4). Casi el mismo número (2^{13} – 4) quedará disponible. A su vez, se pueden emplear estas direcciones para crear nuevas redes. Por ejemplo, puede utilizarse este "residuo" para crear 31 redes, cada una de ellas con el mismo tamaño de una red de clase C, y para generar varias redes más pequeñas. Evidentemente, puede reelegirse otra división; sin embargo, es claro que cuando se utilizan máscaras de longitudes variables, un administrador tiene más capacidad de usar con eficacia todas las direcciones disponibles.

La figura 18.13 muestra la red de ejemplo estructurada al emplear máscaras de longitud variable.

Considérese cómo el ruteador R2 procesa los paquetes que llegan a sus interfases (tabla 18.9).

Supóngase que el paquete que llega al ruteador R2 tiene la dirección de destino *129.44.192.5*. Como esta tabla no contiene rutas específicas, el ruteador procede con la se-

1 byte	2 bytes	3 bytes		4 bytes	
Campo de número de subred de clase B (inalterable) 129	44	Subred		Campo de direcciones del host (espacio de dirección)	
10000001	00101100	0	0000000	00000000	Red 129.44.0.0 Máscara 255.255.128.0
⋮	⋮		⋮		
10000001	00101100	0	1111111	11111110	Número de hosts 2^{15}
10000001	00101100	0	1111111	11111111	
10000001	00101100	1	0 000000	00000000	Red 129.44.128.0 Máscara 255.255.192.0
⋮	⋮		⋮	⋮	
10000001	00101100	1	0 111111	11111111	Número de hosts 2^{14}
10000001	00101100	1	1 000000	00000 000	Red auxiliar 129.44.192.0 Máscara 255.255.255.248
10000001	00101100	1	1 000000	00000 001	
....	....	.	. ...	...	
10000001	00101100	1	1 000000	00000 110	Número de hosts 8
10000001	00101100	1	1 000000	00000 111	
Intervalo de direcciones (2^{13} – 8), disponible para nuevas redes					
10000001	00101100	1	1 1 00000	00000000	Red 129.44.224.0 Máscara 255.255.224.0
⋮	⋮	⋮	⋮ ⋮	⋮	Número de hosts 2^{13}
10000001	00101100	1	1 1 11111111	111111	

Espacio de dirección 2^{16}

FIGURA 18.12 División del espacio de dirección de la red de clase B (129.44.0.0) en redes de diferentes tamaños en las que se utilizan máscaras de longitud variable.

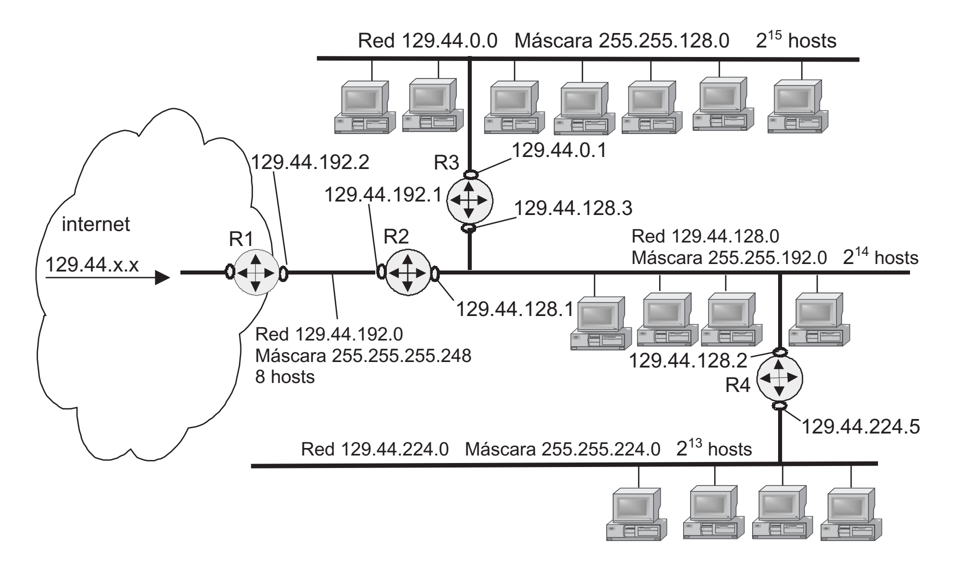


FIGURA 18.13 Estructura de la red en la que se emplean máscaras de longitud variable.

gunda fase de la búsqueda de la tabla: con el análisis secuencial de todas las filas para una dirección de destino coincidente:

(129.44.192.5) AND (255.255.128.0) = 129.44.128.0: no coinciden las direcciones de destino

TABLA 18.9 Tabla de enrutamiento del ruteador R2 en la red con máscaras de longitud variable

Dirección de destino	Máscara	Dirección del siguiente ruteador	Dirección del puerto	Distancia
129.44.0.0	255.255.128.0	129.44.128.3	129.44.128.1	1
129.44.128.0	255.255.192.0	129.44.128.1	129.44.128.1	Conectado
129.44.192.0	255.255.255.248	129.44.192.1	129.44.192.1	Conectado
129.44.224.0	255.255.224.0	129.44.128.2	129.44.128.1	1
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–

(129.44.192.5) AND (255.255.192.0) = 129.44.192.0: no coinciden las direcciones de destino
(129.44.192.5) AND (255.255.255.248) = 129.44.192.0: coinciden las direcciones de destino
(129.44.192.5) AND (255.255.244.0) = 129.44.192.0: no coinciden las direcciones de destino

De este modo, hubo una coincidencia en una fila. El paquete se enviará a la red directamente conectada al ruteador actual: hacia la interfase de salida 129.44.192.1.

Si el paquete con la dirección *129.44.192.1* llega desde la red externa y el ruteador R1 funciona sin utilizar máscaras, el paquete se pasará al ruteador R2 y será devuelto a la red de tránsito. Como es obvio, esto es ineficaz.

El enrutamiento será más eficaz si en la tabla del ruteador R1 todas las rutas se especifican con máscaras de longitud variable. El fragmento de una tabla así se encuentra en la tabla 18.10. El primero de los dos registros proporcionados en esta tabla señala que todos los paquetes que tienen direcciones de destino a partir de 129.44 tienen que pasarse al ruteador R2. Este registro lleva a cabo la **agregación de dirección** para todas las subredes creadas con base en la red 129.44.0.0. El segundo registro especifica que entre todas las posibles subredes de la red 129.44.0.0, existe una red, 129.44.192.0/30, a la que los paquetes pueden cambiarse directamente desde pasar a través del ruteador R2.

TABLA 18.10 Fragmento de la tabla de enrutamiento del ruteador R1

Dirección de destino	Máscara	Dirección del siguiente ruteador	Dirección del puerto	Distancia
....	....	....	....	....
129.44.0.0	255.255.0.0	129.44.192.1	129.44.192.2	2
129.44.192.0	255.255.255.252	129.44.192.2	129.44.192.2	Conectado
....	....	....	....	....

NOTA *Cuando se utiliza el mecanismo de máscaras, únicamente la dirección IP de destino es pasada en paquetes IP, sin la máscara de la red de destino. Por lo tanto, es imposible encontrar cuál parte de la dirección IP del paquete entregado se relaciona con el número de red y cuál parte se asocia al número de host. Si las máscaras en todas las subredes tienen el mismo tamaño, esto no causará ningún problema. No obstante, si las máscaras de longitudes variables se utilizan para la elaboración de subredes, el ruteador deberá tener algún mecanismo que permita detectar cuáles máscaras corresponden a las direcciones de la red. Para este propósito, se usan los protocolos de enrutamiento, los cuales conducen información acerca de las direcciones de la red junto con información en máscaras de red correspondientes a estos números entre los ruteadores. La lista de tales protocolos incluye RIPv2 y OSPF. Como se relaciona con RIP, no conduce máscaras de red. Por lo tanto, este protocolo no es adecuado para emplear máscaras de longitudes variables.*

18.4.4 Traslape de espacios de dirección

Cuando comienza la configuración de las interfases de red y la creación de la tabla de enrutamiento, para un administrador no es complicado administrar máscaras por primera vez. Esto ocurre de manera bastante temprana en la planeación de la red, misma que implica determinar el número de redes que se incluirán en toda la red de la compañía, evaluar el número requerido de direcciones para cada red, obtener de nuevo un conjunto de direcciones del proveedor y distribuir el espacio de dirección disponible entre las redes. Esta última tarea suele no ser trivial, especialmente cuando hay escasez de direcciones.

Considérese el ejemplo de la máscara empleada para organizar **espacios de dirección con traslape**.

Supóngase que la gerencia de alguna compañía ha solicitado un conjunto de direcciones suficiente para crear una red, cuya estructura se muestra en la figura 18.14. La red cliente incluye tres subredes, dos de las cuales son internas a nivel de departamento: Ethernet destinada para 600 usuarios y una red Token Ring para 200 usuarios. La compañía también previene la presencia de una red por separado, incluidos 10 hosts, cuyo objetivo principal es proporcionar información a clientes potenciales en el modo de acceso público. Tales secciones de una red corporativa, en la que se localizan servidores web, servidores FTP y otras fuentes de información pública, se conocen por lo general como **zonas desmilitarizadas** (**DMZ**, por sus siglas para **DeMilitarized Zones**). Además, se requiere una red adicional que contenga sólo dos hosts para conexión con el proveedor de servicio. De este modo, el número total de direcciones indispensables para asignar interfases de red es 812. Aparte de ello, es necesario asegurar que el conjunto de direcciones disponibles incluya direcciones de transmisión que tengan sólo unos y otras con únicamente ceros. Debido a que cualquier dirección de red de todos los hosts debe tener los mismos prefijos, es evidente que el número mínimo de direcciones requeridas por el cliente para construir una red así puede diferir significativamente de 812, lo cual se obtuvo mediante una suma simple.

En este ejemplo, el proveedor decide asignar al cliente un conjunto de dirección continuo que contenga 1 024 direcciones. Se seleccionó el número 1 024 porque es la potencia de dos (2^{10} = 1 024) más cercana al número requerido de direcciones. El proveedor busca el área de longitud tal en el espacio de dirección disponible: 131.57.0.0/16. Observe que por lo regular una parte de este espacio ya está asignado a otros clientes, como se muestra en la figura 18.15. Designe los intervalos de dirección atribuidos a los clientes como S1, S2 y S3. El proveedor encuentra un intervalo continuo entre las direcciones disponibles que no se ha distribuido todavía. El tamaño de este intervalo es de 1 024 direcciones y la dirección de

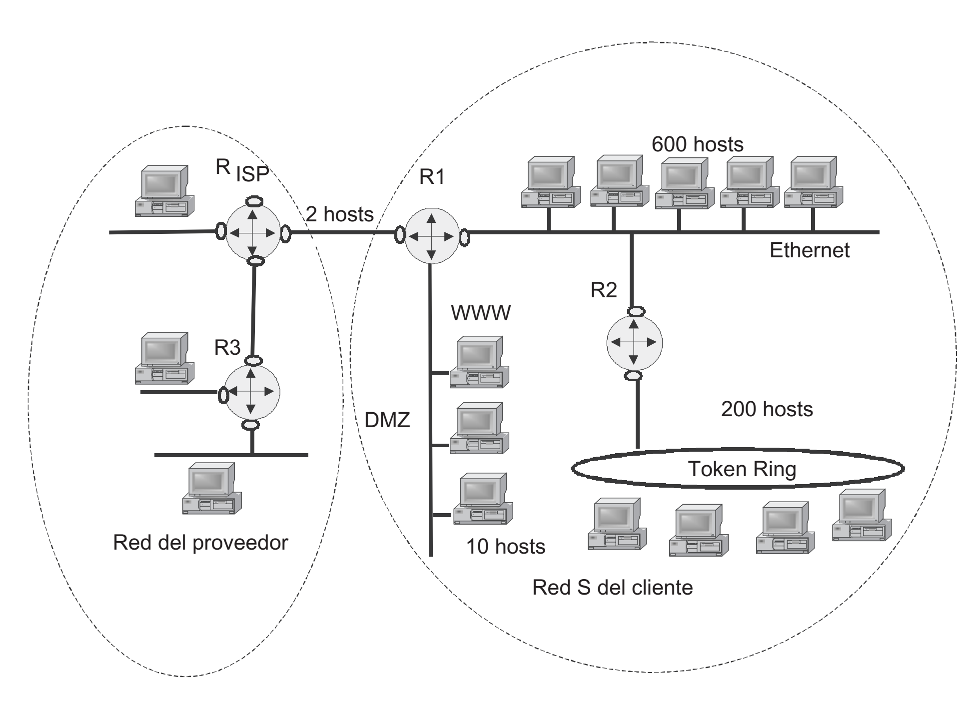


FIGURA 18.14 Redes del proveedor y el cliente.

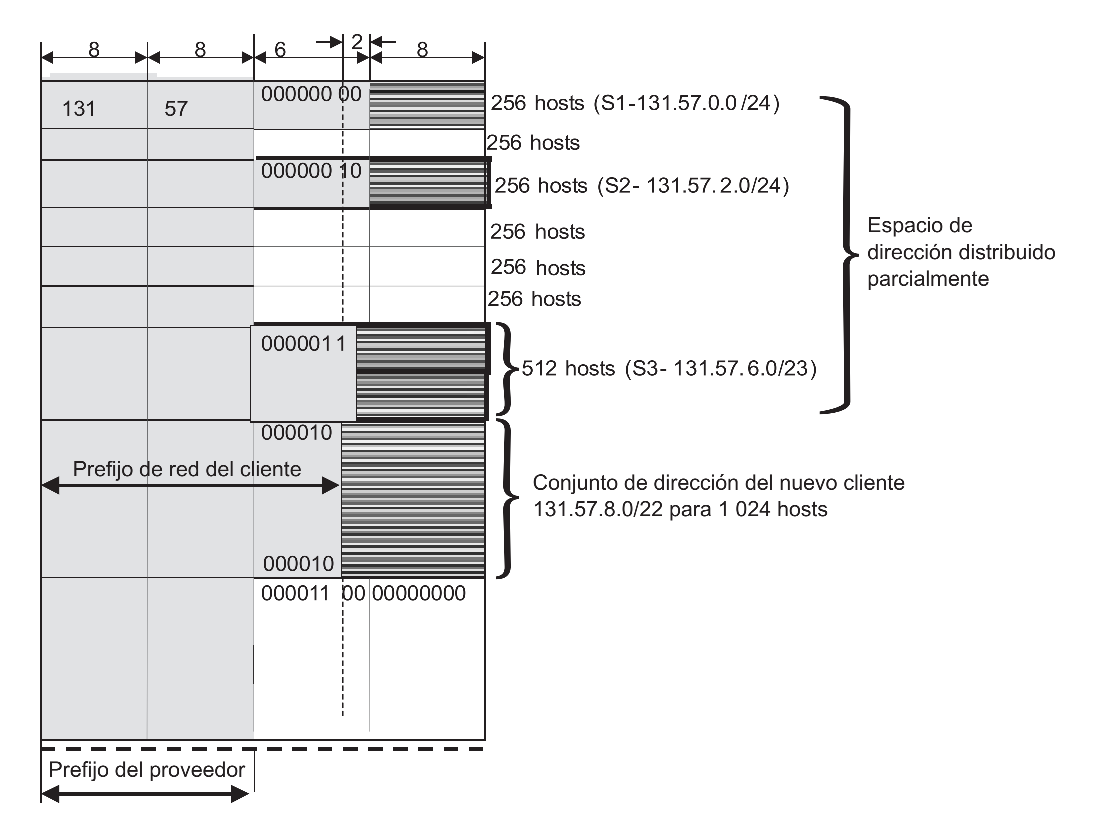


FIGURA 18.15 Espacio de dirección del proveedor.

inicio del intervalo es un múltiplo del tamaño de este intervalo. Así, el nuevo cliente obtendrá el conjunto de dirección 131.57.8.0/22, designado como S en la ilustración.

Entonces, comienza la etapa más difícil de la planeación de la red. Es necesario distribuir el conjunto de dirección S obtenido del proveedor entre cuatro redes de la compañía. En primer lugar, el administrador decide asignar todo el conjunto de dirección 131.57.8.0/22 a la red más grande, Ethernet, que contiene 600 nodos (figura 18.16). El número de red asignado a esta red coincide con el número de reto obtenido del proveedor. Muy bien, ¿qué debería hacer el administrador con las tres redes restantes? El administrador tiene presente que Ethernet requiere únicamente 600 direcciones. De las 424 direcciones restantes, el administrador reúne "a duras penas" 256 para la red Token Ring. El administrador aprovecha que Token Ring necesita sólo 200 direcciones y entonces "recorta" dos secciones de ella: 131.57.9.16/28 con 16 direcciones para organizar una DMZ y 131.57.9.32/30 con cuatro direcciones para la red que conecta la compañía a la red del ISP. Como resultado, todas las redes de esta compañía han sido asignadas a un número suficiente de direcciones (a veces incluso de manera redundante). `

La etapa siguiente consiste en configurar las interfases de red de los nodos terminales y ruteadores. Cada interfase está configurada con su dirección IP y su máscara apropiada. La figura 18.17 muestra la red del cliente configurada.

Una vez configuradas todas las interfases de la red, es necesario crear una tabla de enrutamiento para los ruteadores R1 y R2 del cliente. Pueden ser generadas automáticamente o de forma manual por un administrador. La tabla 18.11 indica la tabla de enrutamiento del ruteador R2.

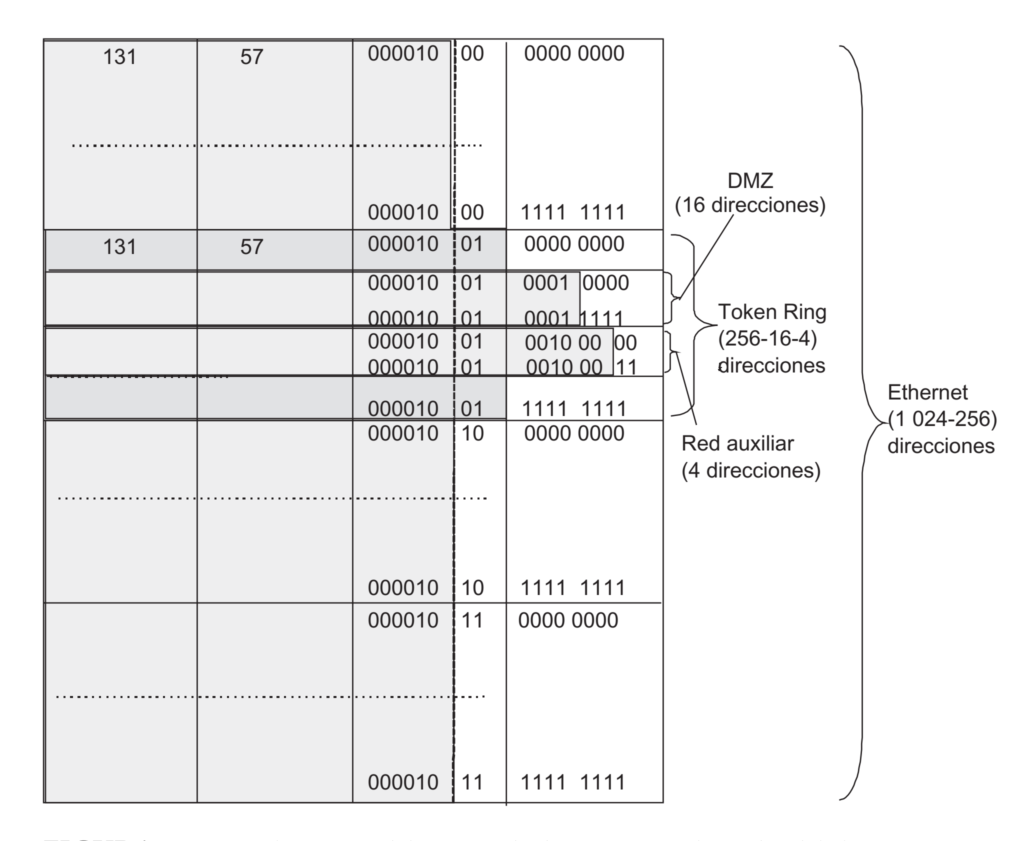


FIGURA 18.16 Planeación del espacio de dirección para las redes del cliente.

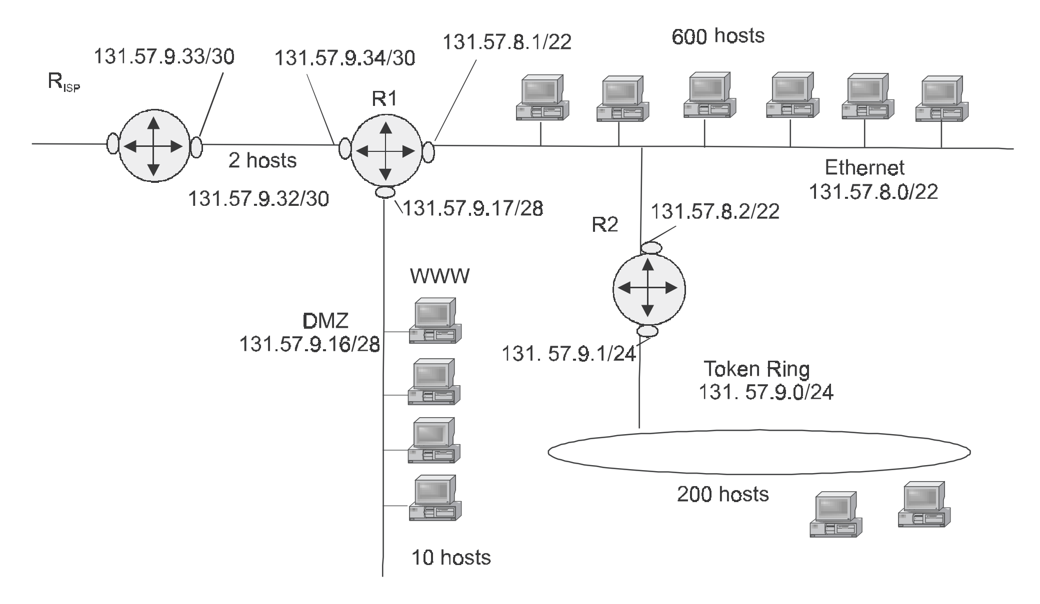


FIGURA 18.17 Configuración de la red del cliente.

TABLA 18.11 Tabla de enrutamiento del ruteador R2

Dirección de destino	Máscara	Dirección del siguiente ruteador	Dirección de la interfase de salida	Distancia
131.57.8.0	255.255.252.0	131.57.8.2	131.57.8.2	Conectado
131.57.8.0	255.255.255.0	131.57.9.1	131.57.9.1	Conectado
131.57.8.16	255.255.255.240	131.57.8.1	131.57.8.2	1
131.57.8.32	255.255.255.252	131.57.8.1	131.57.8.2	1

Dicha tabla no contiene una ruta predeterminada, lo cual significa que todos los paquetes destinados para las redes que tengan direcciones que no estén especificadas explícitamente en la tabla serán descartados por este ruteador.

Por ejemplo, supóngase que el paquete con dirección de destino 131.57.9.29 llega al ruteador R2. Como resultado de la búsqueda en la tabla, usted obtendrá los siguientes resultados para cada fila de la tabla:

(131.57.9.29) AND (255.255.252.0) = 131.57.8.0: coincide

(131.57.9.29) AND (255.255.255.0) = 131.57.9.0: coincide

(131.57.9.29) AND (255.255.255.240) = 131.57.9.16: coincide

(131.57.9.29) AND (255.255.255.252) = 131.57.9.28: no coincide

De acuerdo con el algoritmo de búsqueda de la tabla de enrutamiento, si existen varias coincidencias, se elegirá la ruta de la fila en la que la dirección de destino del paquete que coincide con la dirección de destino de la tabla tenga la longitud máxima. De este modo, se definirá que el paquete con la dirección 131.57.9.29 será dirigido hacia la red DMZ.

18.4.5 Enrutamiento y CIDR

En los últimos años ha habido múltiples cambios en Internet: el número de hosts y redes creció de manera considerable, la intensidad del tráfico se incrementó y el tipo de datos transmitidos cambió. Debido a la intersección de los protocolos de enrutamiento, el intercambio de mensajes portadores de información acerca de actualizaciones de tablas de enrutamiento comenzó a generar fallas de los ruteadores troncales. Esto ocurrió debido a la congestión provocada por el procesamiento de una gran cantidad de información de control. Por ejemplo, las tablas de enrutamiento de los ruteadores troncales de Internet en la actualidad pueden contener cientos o incluso miles de rutas.

Para superar ese problema, se diseñó la tecnología del **enrutamiento de interdominio sin clase (CIDR**, por sus siglas para **Classless InterDomain Routing**).

La idea principal del CIDR es la siguiente: cada ISP debe asignarse a un intervalo continuo en el espacio de dirección IP. Cuando se utiliza un enfoque así, las direcciones de todas las redes de cada proveedor de servicios tendrán una parte más significativa en común: el **prefijo**. Por lo tanto, el enrutamiento en los troncales de Internet puede llevarse a cabo con base en los prefijos en lugar de en las direcciones de red calificadas completamente. Esto significa que en vez de varios registros, un registro por cada red, será suficiente tener uno solo para el conjunto de redes que tienen prefijos coincidentes. La agregación de dirección disminuirá el volumen de las tablas de enrutamiento en los ruteadores de todos niveles. En consecuencia, los ruteadores funcionarán con más rapidez y el ancho de banda de Internet se verá incrementado.

En líneas anteriores se dieron algunos ejemplos de cómo los administradores de redes corporativas utilizaban máscaras para dividir un conjunto de dirección continua obtenido de un ISP en varias partes de modo que se empleara para estructurar sus redes. Una variante así que utilizaba máscaras se conoce como **elaboración de subredes** (RFC 950).

Al mismo tiempo, el uso de máscaras para dividir una red en subredes también tiene un efecto inverso: la **agregación de redes**. En términos sencillos, a fin de dirigir todo el tráfico entrante en la red corporativa dividida en subredes, es suficiente tener solamente un registro en todos los ruteadores externos, el cual debe especificar el prefijo común para todas estas redes como una dirección de destino. Para especificar la frontera correcta del prefijo se utiliza una máscara apropiada: ésta es la **elaboración de superredes** o "**superneteo**", una operación inversa a la elaboración de subredes. La elaboración de superredes significa que las máscaras se utilizan para agregar varias redes en una sola mayor.

Al observar de nuevo la figura 18.15, se muestra el espacio de dirección del ISP con los intervalos de direcciones S1, S2, S3 y S asignados para cuatro clientes. Este ejemplo también aparece en la figura 18.18. Como resultado de la agregación de redes de cliente en la tabla 18.12 del ruteador R_{ISP}, se asignará una fila a cada cliente independiente del número de subredes que ellos han organizado en sus redes. Por ejemplo, en vez de proporcionar cuatro rutas para siete redes del cliente S, la tabla contiene sólo una ruta común para todas estas redes.

Para un proveedor de alto nivel de soporte a clientes que utilice el ruteador $R_{externo}$, los esfuerzos del proveedor local para dividir su espacio de dirección no serán evidentes. El registro 131.57.0.0 con la máscara 255.255.0.0 describe por completo las redes del proveedor local en el ruteador $R_{externo}$.

Así, la tecnología CIDR proporciona las soluciones siguientes:

- Mayor uso compartido del espacio de dirección. Con la tecnología CIDR, los proveedores pueden "seccionar" el espacio de dirección asignado a ellos de acuerdo con los reque-

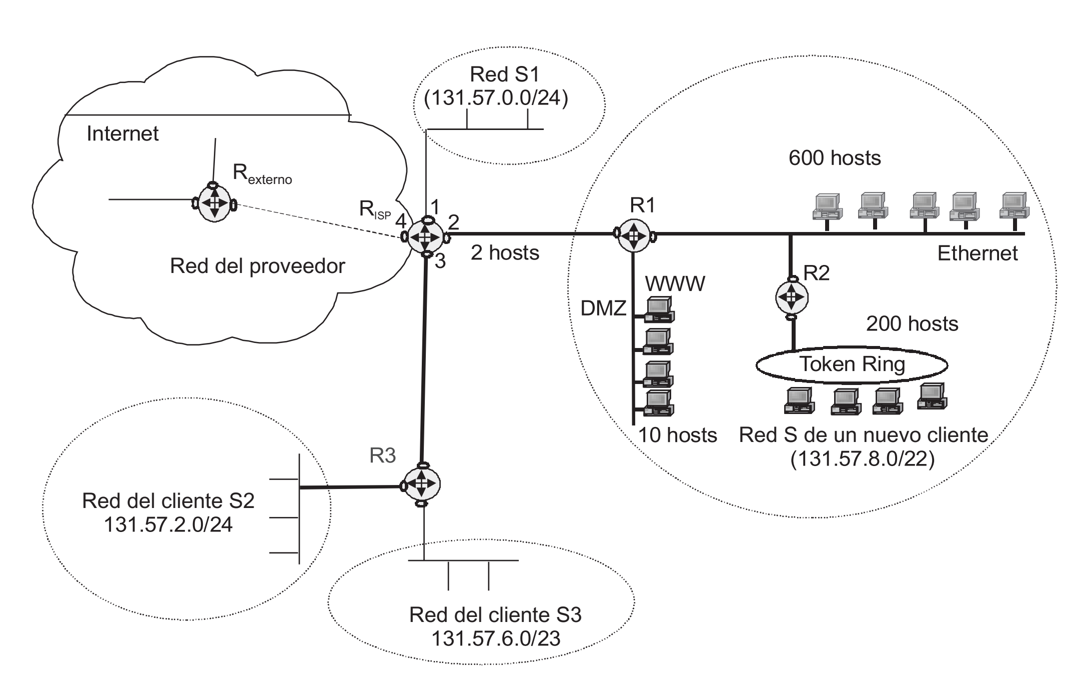


FIGURA 18.18 Elaboración de superredes (*supernetting*).

TABLA 18.12 Tabla de enrutamiento del ruteador R_{ISP}

Dirección de destino	Máscara	Siguiente ruteador	Número de la interfase de salida	Distancia
131.57.0.0 (S1)	255.255.255.0	–	1	Conectado
131.57.2.0 (S2)	255.255.255.0	R3	3	1
131.57.6.0 (S3)	255.255.254.0	R3	3	1
131.57.8.0 (S)	255.255.252.0	–	2	1
Predeterminado	0.0.0.0	$R_{externo}$	4	–

rimientos de cada cliente. Al mismo tiempo, los clientes tendrán cierta reserva para el futuro.

- Un número disminuido de registros en tablas de enrutamiento debido a la agregación de ruta. Así, un solo registro en la tabla de enrutamiento puede representar un gran número de redes. Si todos los ISP siguen la estrategia CIDR, la ganancia sería evidente en especial en los ruteadores troncales.

La localización de direcciones no sólo es un requisito obligatorio del uso eficaz de CIDR, sino también significa que las direcciones con prefijos coincidentes sean asignadas a redes localizadas de manera cercana entre sí. La agregación de tráfico es posible sólo cuando se ha observado esta condición.

Por desgracia, la distribución de dirección es aleatoria en muchos aspectos. La reasignación de números de red es un método fundamental para enfocar este problema. No obstante, este procedimiento requiere inversiones en tiempo y dinero. Por lo tanto, para llevarla a cabo, es necesario estimular a los usuarios de alguna manera. Un estímulo así puede incluir la facturación por cada fila en la tabla de enrutamiento o por el número de hosts en la red. El primer requerimiento hace reconsiderar al cliente la idea de obtener direcciones del proveedor que permitan que el enrutamiento de tráfico en su red esté basado en el prefijo de la red. Cuando se consigue esto, los registros con los números de red de la compañía ya no se presentarán en ruteadores troncales. El requerimiento para pagar por cada dirección de host también puede motivar al usuario a volver a numerar y obtener la cantidad de direcciones que no excedan de manera significativa el número requerido.

La tecnología CIDR se utiliza con éxito en la versión actual de IP, IPv4 y también es soportada por protocolos de enrutamiento tales como OSPF, RIPv2 y BGP4 (principalmente en los ruteadores troncales de Internet). Las características específicas del uso de CIDR en la nueva versión de IP, IPv6, se analizarán más adelante en la sección dedicada a IPv6.

18.5 FRAGMENTACIÓN DE PAQUETES IP

PALABRAS CLAVE: fragmentación, fragmento, MTU, redes heterogéneas, identificador, TTL, bandera DF, bandera MF, desplazamiento o compensación, mejor esfuerzo, ensamblado, paquete IP, trama de tecnología local y temporizador.

Una característica importante de IP, que difiere de los otros protocolos de red (como IPX), es su capacidad para llevar a cabo **fragmentación dinámica de paquetes** cuando se transmiten paquetes de red en redes. La fragmentación es necesaria si estas redes tienen diferentes longitudes máximas de los campos de datos de la trama (unidad de transmisión máxima o MTU). La capacidad de fragmentación de paquetes característica de IP ha mejorado en muchos aspectos la escalabilidad de la tecnología TCP/IP.

18.5.1 MTU como parámetro tecnológico

En primer lugar, cabe señalar la diferencia entre la fragmentación del mensaje en el nodo fuente y la fragmentación dinámica de mensajes en los nodos de tránsito de la red: ruteadores. Prácticamente en todas las pilas de protocolo existen protocolos responsables de dividir mensajes de capa de aplicación en fragmentos tales que se ajusten a las tramas de capa de enlace de datos. Para este propósito, analizan el equipo de la tecnología subyacente y definen su MTU.

En la pila TCP/IP, este problema es resuelto por TCP, que divide el flujo de bytes que le transmiten de la capa de aplicación en segmentos del tamaño requerido (por ejemplo, 1 460 bytes si el protocolo Ethernet se utiliza como la tecnología subyacente de la red). Por ende, el IP del **remitente** por lo regular no emplea sus capacidades de fragmentación. Sin embargo, la situación resulta distinta para los ruteadores cuando es necesario pasar el paquete desde la red actual a otra que tenga un MTU más pequeño. En este caso, se utilizan las capacidades de fragmentación de IP.

De la tabla 18.13, es claro que los valores MTU para las tecnologías más conocidas son significativamente distintos. Esto significa que la fragmentación es una práctica común en las redes heterogéneas contemporáneas.

TABLA 18.13 Valores típicos MTU

Tecnología	MTU
DIX Ethernet	1 500 bytes
Ethernet 802.3	1 492 bytes
Token Ring (IBM, 16 Mbps)	17 914 bytes
Token Ring (802.5, 4 Mbps)	1 464 bytes
FDDI	4 352 bytes
X.25	576 bytes

18.5.2 Parámetros de fragmentación

La idea principal de la fragmentación consiste en dividir el paquete que llega desde la red con la MTU más grande en paquetes más pequeños, **fragmentos**, si este paquete tiene que ser dirigido hacia la red con la MTU más pequeña. A medida que los fragmentos viajan a través de la red, son divididos una vez más en alguno de los ruteadores de tránsito. A cada fragmento se le debe suministrar un encabezado IP de valor completo.

Algunos de los campos de encabezado, como el *identificador*, *TTL*, las *banderas DF* y *MF*, así como el *desplazamiento*, están destinados directamente al procedimiento de ensamblar fragmentos en el mensaje fuente:

- El receptor de un fragmento utiliza el *campo del identificador para reconocer todos los fragmentos del mismo paquete*. El módulo IP que envía el paquete rellena el campo del identificador con el valor que debe ser único para el par actual "emisor-receptor". Esta condición debe observarse durante todo el tiempo que este paquete (o cualquiera de sus fragmentos) exista en la interred IP. Para asegurar que se cumplan estas condiciones, la entidad IP que envía los paquetes puede rastrear los identificadores asignados. Por ejemplo, esto puede hacerse mediante el respaldo de la tabla en la que cada registro se relaciona con un host de destino individual con el que se ha establecido la conexión. Cada registro de una tabla de esta naturaleza contiene el último valor TTL del paquete en la red IP. Sin embargo, debido a que el campo del identificador permite 65 536 valores diferentes, algunas implementaciones de IP eligen aleatoriamente identificadores de este intervalo, confiando en la alta probabilidad de que el identificador será único durante la transmisión del paquete.
- El remitente especifica el *TTL* durante el cual el paquete puede existir en la red.
- El campo de *desplazamiento o compensación* de un fragmento de paquete informa al receptor acerca de la posición de este fragmento en el paquete fuente. De este modo, el primer fragmento siempre tendrá desplazamiento o compensación cero. Si el paquete no está fragmentado, el campo de desplazamiento también tendrá el valor cero.
- La bandera *MF* establecida a 1 indica que el fragmento que acaba de llegar no es el último. La entidad IP que envía un paquete no fragmentado establece la bandera *MF* a cero.

- La bandera *DF* establecida a 1 indica que el paquete actual no debe ser fragmentado bajo ninguna condición. Si el paquete marcado como aquel que no debe ser fragmentado no puede alcanzar el nodo de destino sin fragmentación, la entidad IP lo descartará y enviará un mensaje ICMP apropiado al emisor o remitente.

NOTA *La posibilidad de bloquear la fragmentación de paquete puede ayudar en algunos casos a que las aplicaciones corran más rápido. Para conseguir esto, primero se debe investigar la red y determinar el máximo tamaño del paquete que puede viajar a lo largo de la trayectoria sin fragmentación. Después de ello, deberán utilizarse únicamente los paquetes que no excedan este tamaño. Dicha característica también puede emplearse para evitar la fragmentación cuando los recursos del host de destino no son suficientes para ensamblar los fragmentos.*

18.5.3 Procedimientos de fragmentación y paquetes de ensamble

En primer lugar considérese el procedimiento de **fragmentación**. Antes de dividir en fragmentos el paquete recién llegado, el IP instalado en el ruteador asigna varios búferes o memorias temporales para nuevos fragmentos.

Entonces se copia el contenido de algunos campos del encabezado IP desde el paquete original en estos búferes, con lo cual se crean encabezados IP "falsos" para los nuevos paquetes fragmentados. Algunos parámetros del encabezado IP se copian en los encabezados de todos los fragmentos, mientras que otros permanecen solamente en el encabezado del primer fragmento. El proceso de fragmentación puede modificar los valores de algunos campos de encabezados IP de los fragmentos que corresponden al encabezado IP del paquete original. De esta manera, cada fragmento tiene su propio valor de suma verificadora de encabezado, desplazamiento de fragmento y longitud total de paquete. En todos los paquetes (excepto el último), la bandera *MF* se establece a uno, pero en el último fragmento se establece a cero.

El contenido del campo de datos de cada fragmento se formará al dividir el contenido del campo de datos del paquete original. Con todo esto en actividad, deben cumplirse las condiciones siguientes: en primer lugar, el tamaño del fragmento (el encabezado IP más el campo de datos) no debe exceder la MTU de la tecnología subyacente. En segundo, el tamaño del campo de datos de cada fragmento con excepción del último debe ser un múltiplo de 8 bytes. El tamaño de la última parte de los datos es igual al residuo.

Ahora considérese cómo se reensamblan los paquetes fragmentados. Este procedimiento tiene lugar en el host de destino.

NOTA *Observe que los ruteadores IP no ensamblan fragmentos del paquete en paquetes más grandes, incluso si a lo largo de sus trayectorias existen algunas redes que permitan tal agregación. La razón para tal comportamiento es simple. Diferentes fragmentos del mismo mensaje pueden viajar a lo largo de rutas distintas en la interred. En consecuencia, no hay garantía de que todos los fragmentos viajarán a través del mismo ruteador.*

De este modo, para cada paquete fragmentado se asigna un búfer especial en el host de destino, en el cual la entidad IP coloca los fragmentos IP que tienen direcciones fuente, direcciones de destino y valores de los campos de *identificador* y *protocolo* coincidentes. Todos estos atributos especifican que dichos paquetes son fragmentos del mismo paquete original. El proceso de ensamblado consta de la colocación de los datos de cada fragmento en la posición especificada por el campo de *compensación* o *desplazamiento* del encabezado del paquete.

Cuando el primer fragmento del paquete original llega al host de destino, este host inicia el temporizador o cronómetro de reensamblado que determina el tiempo máximo durante el cual se permite esperar la llegada de otros fragmentos de este paquete. En diferentes implementaciones de IP, se aplican diversas reglas de selección de este periodo de espera. Por ejemplo, el temporizador puede establecerse al valor fijado (de 60 a 120 segundos) recomendado por RFC. Como regla, tal intervalo es suficiente para la entrega del paquete desde el emisor hasta el receptor. Otras implementaciones podrán determinar este intervalo si se utilizan algoritmos adaptativos al medir el tiempo en la red y evaluar de manera estadística el tiempo de las llegadas de fragmentos. Finalmente, podrá seleccionarse el tiempo de espera con base en los valores TTL conducidos en los fragmentos recibidos. Este último enfoque está basado en la idea de que no tiene sentido esperar que lleguen otros fragmentos si el TTL de uno de los fragmentos recibidos ha expirado.

NOTA *Si al menos un fragmento del paquete no ha llegado a tiempo al host de destino (a tiempo significa antes de que termine el temporizador), no se toman acciones para la duplicación del fragmento perdido y se descartan todos los fragmentos recibidos. El host de destino envía un mensaje de error ICMP al emisor o remitente. Este comportamiento de IP corresponde a su plan del "mejor esfuerzo" (es decir, el protocolo realiza su mejor esfuerzo para entregarle paquete pero no da garantías).*

La falta de intervalos en blanco ("agujeros") en el campo de datos y la llegada del último fragmento (*MF = 0*) indican que se ha completado el proceso de ensamble. Después de que se han ensamblado los datos, se podrán transmitir a un protocolo de capa superior, como TCP.

18.5.4 Ejemplo de fragmentación

Supóngase que la fragmentación se llevará a cabo en el ruteador (figura 18.19).

Considérese también que el host emisor está conectado a la red que tiene una MTU de 17 914 bytes, por ejemplo: una red Token Ring. Como regla, la capa de transporte conoce la MTU de la tecnología subyacente y elige el tamaño del segmento. Supóngase que en este ejemplo, el mensaje de 6 600 bytes se pasa desde la capa de transporte hasta la capa IP, la cual forma el campo de datos del paquete IP con base en este mensaje y le suministra el encabezado. Debe ponerse atención especial a la manera de rellenar los campos del encabezado relacionados con la fragmentación del paquete. En primer lugar, se asigna al paquete un identificador único, por ejemplo: 12 456. En segundo lugar, como el paquete todavía no ha sido fragmentado, el campo de *desplazamiento* (*offset*) se establece a cero, mientras que la bandera *MF* también se establece a cero para especificar que no hay fragmentos por seguir. En tercer lugar, la bandera *DF* se establece a 1, lo cual significa que este paquete puede ser fragmentado. La longitud total del paquete IP es de 6 600 + 20 (tamaño del encabezado IP), es decir, 6 620 bytes. La longitud de este paquete cabe dentro del campo de datos de la trama Token Ring. A continuación la entidad IP del host emisor pasa esta trama a su interfase de red, que envía las tramas hacia el siguiente ruteador.

Después de que la trama pasa la capa de red de la interfase de red del ruteador y es despojada del encabezado Token Ring, la entidad IP del ruteador recuperará la dirección de la red de destino a partir del paquete. Mediante esta dirección, determinará que el paquete IP recién llegado debe pasarse a la red Ethernet, la cual tiene una MTU de 1 492. Este valor es mucho más pequeño que el tamaño del paquete que llegó a la interfase de entrada. En consecuencia, debe ser fragmentado el paquete IP. El ruteador recuperará el campo de datos del paquete y

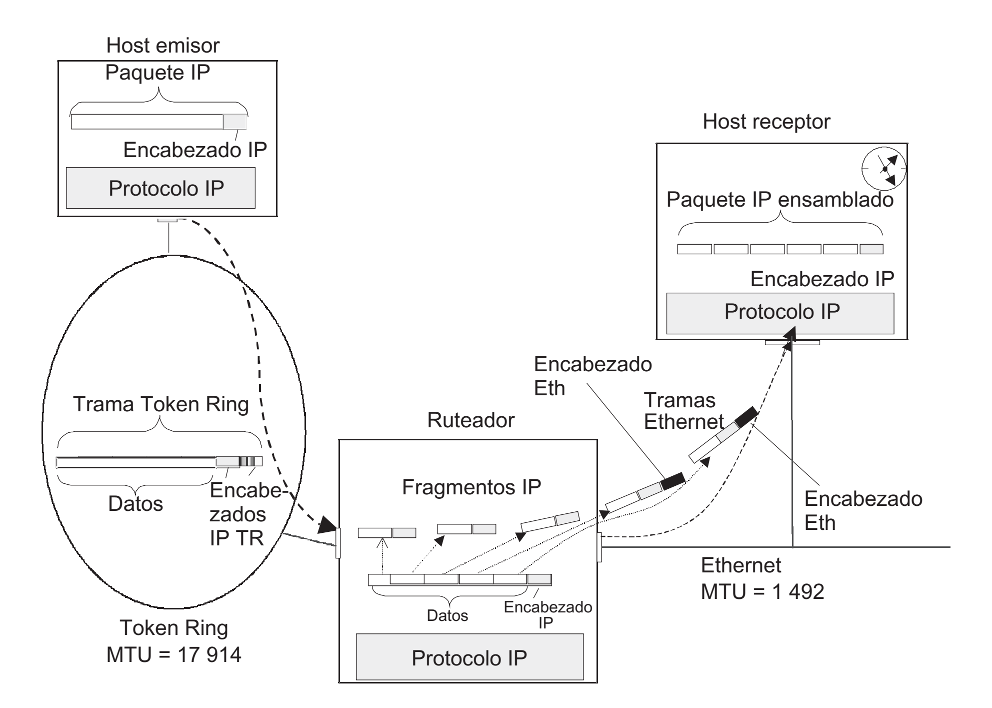


FIGURA 18.19 Fragmentación.

lo dividirá en partes de las siguientes dimensiones: cuatro fragmentos que contienen 1 400 bytes cada uno y un fragmento de 1 000 bytes. Obsérvese que cada fragmento de datos es un múltiplo de ocho. Entonces, la entidad IP forma nuevos paquetes IP, cuatro de los cuales tendrán la longitud de 1 400 + 20 = 1 420 bytes; la longitud del último paquete será de 1 000 + 20 = 1 020. Estos valores son más pequeños que 1 500 bytes; por lo tanto, dichos paquetes cabrán dentro de los campos de datos de las tramas Ethernet.

Como resultado, el host de destino conectado a Ethernet recibirá cinco paquetes IP con el identificador común 12 456. Si estos paquetes llegan dentro de un tiempo que no exceda el valor del tiempo de espera, el IP que se ejecuta en el host de destino puede ensamblar el mensaje original. Si estos paquetes llegan en un orden diferente del orden en el que fueron enviados, el campo de *desplazamiento* (*offset*) especificará el orden correcto para su ensamblado.

18.6 IPV6

PALABRAS CLAVE: IPv6, protocolo de Internet de la siguiente generación (IPng, IP next generation), Internet, medios masivos, método de direccionamiento escalable, QoS, seguridad, IPSec, forma hexadecimal de dirección, prefijo de formato (FP, Format Prefix), unidirigido (unicast), multicast, transmisión o difusión (broadcast), enviado a cualquier nodo (anycast), dirección privada, dirección de enlace local, dirección de sitio local, dirección única agregada local, agregación de alto nivel (TLA, Top-Level Aggregation), agregación del siguiente nivel (NLA, Next-Level Aggregation), agregación de nivel local (SLA, Site-Level Aggregation), dirección IPv6 mapeada en IPv4, direcciones IPv6 compatibles con IPv4 y formato de encabezado flexible.

Desde principios de la década de 1990, la pila TCP/IP ha tenido serios problemas. En ese tiempo, Internet era utilizada de manera más activa para propósitos industriales. Por ejemplo, la mayoría de las organizaciones comenzaban a construir sus redes corporativas mediante el uso de Internet como sistema de transporte. También comenzaron a utilizar tecnologías web para tener acceso a información corporativa. Aparte de ello, el comercio electrónico (*e-commerce*) que usaba Internet comenzó a extenderse y esta red se empleaba en medios masivos y en las industrias del entretenimiento, como en la transmisión de audio y video y en juegos interactivos.

Todos estos factores han generado un crecimiento explosivo en el número de hosts de red. A principios de la década de 1990 se conectaban nuevos hosts a Internet cada 30 segundos. En consecuencia, el tipo de tráfico cambió y los requerimientos QoS llegan a ser significativamente más rigurosos.

18.6.1 Direcciones de modernización de la pila TCP/IP

La comunidad de Internet y más adelante toda la industria de las telecomunicaciones comenzaron a resolver los problemas mediante el diseño de nuevos protocolos para la pila TCP/IP, como RSVP, IPSec y MPLS. Sin embargo, incluso en aquel tiempo era evidente para los expertos más afamados que la tecnología TCP/IP no podía mejorarse con sólo agregar nuevos protocolos. Era necesario aventurarse a modernizar el núcleo de la pila IP. La principal justificación para este enfoque fue que algunos problemas no podían ser resueltos sin modificar el formato del paquete IP y sin rehacer la lógica de procesamiento de los campos de encabezado IP. Entre estos problemas, el más urgente era la escasez de direcciones IP disponibles para distribución. Por supuesto, este problema no podía resolverse sin ampliar el tamaño de los campos de dirección fuente y de destino.

La escalabilidad del enrutamiento se convirtió en el blanco más popular para las críticas. El punto era que el rápido crecimiento de la red congestionaba los ruteadores, que aún ahora deben procesar tablas de enrutamiento que contengan información de decenas de miles de registros. También es necesario tener presente que los ruteadores deben realizar diversas tareas auxiliares, como la de fragmentación de paquetes. Se sugirieron algunas soluciones a este problema, pero también se debían hacer cambios en IP.

Junto con funciones agregadas directamente en IP, fue necesario asegurar su estrecha interacción con los nuevos protocolos que llegaron a ser miembros de la pila TCP/IP. Esto también requería agregar campos al encabezado IP. El procesamiento de estos campos tenía que llevarse a cabo con dichos protocolos. Por ejemplo, para asegurar la operación de RSVP, sería deseable introducir el campo de clasificación de flujo dentro del encabezado IP, y para IPSec son necesarios campos especiales para transmisión de datos con el fin de dar soporte a las funciones y garantizar su seguridad.

Como resultado, la comunidad de Internet ha decidido modificar radicalmente IP, para lo cual ha seleccionado los objetivos siguientes como las metas principales de esta modernización:

- Crear un método de direccionamiento escalable.
- Reducir las operaciones realizadas por los ruteadores.
- Proporcionar garantías de calidad del servicio de transporte.
- Asegurar la protección de los datos transmitidos a través de la red.

La investigación activa en el campo de la modernización de IP y el desarrollo de nuevos protocolos asociados con ella se inició en 1992. En ese tiempo, se presentaron diversas ver-

siones alternativas del IP de nueva generación a la comunidad de Internet: IPv7 (diseñado por Ullman), TUBA (Callon), ENCAPS (Hinden), SIP (Deering) y PIP (Francis).

Como resultado del proceso de desarrollo, en 1993 se combinaron proyectos como ENCAPS, SIP y PIP dentro de la estructura de la propuesta común que llegó a conocerse como SIPP. En junio de 1994, dicha propuesta se adoptó como la base para el desarrollo del IP de nueva generación: el **Protocolo de Internet de la siguiente generación (IPng)**. En la actualidad, la abreviatura **IPv6** se utiliza comúnmente para designar la nueva versión de IP.

El documento que registró la llegada de IPv6 es RFC 1752, "The Recommendation for the IP Next Generation Protocol" ("Recomendación para el protocolo IP de la siguiente generación"). En septiembre de 1995, IETF adoptó el conjunto básico de protocolos denominado IPv6. En agosto de 1998 se adoptaron las versiones revisadas de los estándares que determinaban la arquitectura IPv6 común (RFC 2460, "*Internet Protocol, Version 6 [IPv6] Specification*") y sus aspectos por separado tales como el sistema de direccionamiento (RFC 2373,"*IP Version 6 Addressing Architecture*"). La más reciente versión de este estándar que describe la arquitectura de las direcciones IPv6 (RFC 3513) fue adoptada hace relativamente poco: en 2003.

18.6.2 Sistema de direccionamiento escalable

La versión más reciente, la sexta, de IP ha introducido cambios significativos en el sistema de direccionamiento de las redes IP. Estos cambios se relacionan principalmente con el incremento de la *capacidad del bit de dirección*.

Capacidad de dirección de bits. Una dirección IPv6 incluye *128 bits* o *16 bytes*, lo cual proporciona la posibilidad de enumerar un vasto número de hosts: 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 762, 211 y 456. Por ejemplo, la magnitud de este número se ilustra mediante lo siguiente: si este número teóricamente posible de direcciones IP se divide entre todos los habitantes de la Tierra (alrededor de 6 000 millones de personas), cada persona tendrá un número inusitadamente grande de direcciones IP: ¡5.7×10^{28}!

Desde luego, un incremento así de significativo en la magnitud de las direcciones estaba dirigido no para eliminar la escasez de direcciones, sino para mejorar la eficiencia global del funcionamiento de la pila TCP/IP.

> El objetivo principal de la modernización de direccionamiento no fue el incremento mecánico del espacio de direcciones, sino ampliar su funcionalidad a expensas de introducir nuevos campos.

En lugar de dos niveles jerárquicos (número de red y número de host), IPv6 proporciona cuatro niveles de jerarquía, entre los cuales tres niveles se utilizan para identificar redes y un nivel está dedicado para identificar hosts. Debido al mayor número de niveles de jerarquía de dirección, el nuevo protocolo soporta de manera eficaz la tecnología CIDR. Esto, además del sistema mejorado de direccionamiento de grupo y la introducción del nuevo tipo de direcciones, permite a la nueva versión IP disminuir los gastos de enrutamiento.

Presentación de dirección. Los cambios también incluyen algunos puramente cosméticos. Por ejemplo, los diseñadores propusieron reemplazar la forma decimal de la representación de las direcciones IP por su *forma hexadecimal*. Cada cuatro dígitos hexadecimales están separados por el signo de "dos puntos" (:). Por ejemplo, una dirección típica IPv6 ahora tiene el siguiente aspecto: FEDC:0A98:0:0:0:0:7654:3210.

Si la dirección incluye una larga secuencia de ceros, esta notación podrá reducirse. Por ejemplo, la dirección proporcionada con anterioridad puede escribirse de la manera siguiente: FEDC:0A98::7654:3210.

La abreviatura "::" puede emplearse solamente una vez dentro de una dirección. También es posible omitir los ceros iniciales al principio de cada campo de la dirección. Por ejemplo, en lugar de FEDC:0A98::7654:3210, es posible escribir FEDC:A98::7654:3210.

Las redes que soportan ambas versiones de IP (IPv4 e IPv6) permiten usar la notación decimal tradicional para IPv4 para los 4 bytes menos significativos. Para los 12 bytes más significativos, se prefiere el formato hexadecimal: 0:0:0:0:0:FFFF:129.144.52.38 o ::FFFF:129.144.52.38.

Tipos de dirección. La nueva versión, IPv6, atiende las necesidades de los siguientes tipos principales de direcciones: *unidirigida* (*unicast*), *multidirigida* (*multicast*) y *enviada a cualquier nodo* (*anycast*). El tipo de dirección está definido por el valor de varios bits más significativos de la dirección, conocidos como el *prefijo de formato* (FP, *format prefix*).

- Las direcciones del tipo **unidirigidas** o **unicast** definen el identificador único de una interfase individual del nodo terminal o ruteador. El principal objetivo de las direcciones de este tipo generalmente coincide con el propósito de las direcciones únicas en IPv4. Al usar tales direcciones, el protocolo entrega los paquetes a una interfase de red específica del nodo de destino. Sin embargo, en contraste con IPv4, en IPv6 no existen los conceptos de clases de red (A, B, C y D) o de división fija relacionada de la dirección con el número de red y el número de host mediante limitantes de 8 bits. Las direcciones del tipo unidirigida se dividen en varios subtipos que reflejan las situaciones más comunes para las redes contemporáneas.
- Las direcciones del tipo **multidirigidas** o **multicast** forman un grupo semejante a la dirección de grupo IPv4 en su objetivo principal. Tiene el prefijo del formato 1111 1111 e identifica el grupo de interfases que por lo regular se relacionan con diferentes hosts. El paquete con una dirección así se entrega a *todas* las interfases que tienen esa dirección. Las direcciones de tipo multidirigida también se emplean en IPv6 para el reemplazo de **direcciones de transmisión o difusión**. Para este propósito, se introduce una dirección de grupo especial, la cual conecta todas las interfases de la subred.
- Las direcciones del tipo **enviadas a cualquier nodo** o **anycast** son un nuevo tipo de dirección que, de modo semejante al tipo multidirigida, especifica un grupo de interfases. Sin embargo, el paquete con una dirección así se entrega a sólo una de las interfases que pertenecen al grupo. Como regla, ésta es la interfase "más próxima" de acuerdo con la métrica utilizada por los protocolos de enrutamiento. En la sintaxis, una dirección enviada a cualquier nodo no difiere de una dirección unidirigida y se asigna desde el mismo intervalo de dirección de las direcciones unidirigidas. Una dirección del tipo enviada a cualquier nodo puede asignarse únicamente a las interfases del ruteador. Las interfases del ruteador pertenecientes al mismo grupo de enviadas a cualquier nodo tienen direcciones unidirigidas individuales y la dirección enviada a cualquier nodo común. Las direcciones de este tipo están orientadas al enrutamiento fuente o de origen, cuando la ruta para el paquete se halla definida por el emisor al especificar las direcciones IP de todos los ruteadores de tránsito. Por ejemplo, el proveedor puede asignar la misma dirección enviada a cualquier nodo a todos sus ruteadores y especificar dicha dirección a sus suscriptores. Si el cliente desea que los paquetes de su red se transmitan a través de la red perteneciente a ese ISP, será suficiente especificar esa dirección enviada a cualquier nodo en la cadena de las direcciones de ruta fuente. Entonces el paquete se enviará a través del ruteador más cercano de ese proveedor.

- En la sexta versión de IP, semejante a IPv4, existen **direcciones privadas** destinadas para usarse en redes autónomas. En contraste con IPv4, en IPv6 estas direcciones tienen un formato especial. Las direcciones para uso local tienen dos variantes en IPv6:
  - En primer lugar, estas direcciones son para redes no divididas en subredes (y que no utilizan enrutamiento), se conocen como **direcciones de enlace local** y tienen un prefijo de 10 bits con el siguiente formato: 1111 1110 10. La dirección local de enlace contiene solamente el campo de 64 bits del identificador de interfase; todos los otros bits (con excepción del FP) deben establecerse a cero, pues en este caso no hay necesidad de contar con un número de subred.
  - En segundo lugar, dicho grupo incluye direcciones locales destinadas para usarlas en redes divididas en subredes. Tales direcciones se conocen como **direcciones de sitio local**; tienen un prefijo con el formato siguiente: 1111 1110 11 y, en comparación con las direcciones de enlace local, contienen un campo adicional de 2 bytes del número de subred.

El subtipo principal de las direcciones unidirigidas es la dirección única agregada global. Tales direcciones pueden agregarse para simplificar el enrutamiento. En contraste con una dirección única de la versión IPv4, la cual abarca dos campos (número de red y número de host), las direcciones únicas agregadas globales de IPv6 tienen una estructura más complicada que incluye seis campos (figura 18.20).

- El *FP* para direcciones de este tipo comprende 3 bits y tiene el valor de 001.

Los tres tipos siguientes, *agregación de nivel superior* (TLA, *Top-Level Aggregation*), *agregación del nivel siguiente* (NLA, *Next-Level Aggregation*) y *agregación del nivel de sitio* (SLA, *Site-Level Aggregation*), representan tres niveles de identificación de red.

- *TLA* está destinado a la identificación de redes de los mayores proveedores. El valor específico de este prefijo representa la parte común de las direcciones proporcionadas por ese proveedor. El número relativamente pequeño de bits asignados para este campo, 13, se elige en especial para limitar el tamaño de las tablas de enrutamiento en ruteadores troncales de nivel superior de Internet. Este campo permite contar con 8 196 redes de los proveedores de nivel superior. Esto significa que el número de registros que describen las rutas entre estas redes también estará limitado por el valor 8 196, el cual acelerará la operación de los ruteadores troncales. Los siguientes 8 bits están reservados para uso futuro, con el fin de extender el campo *TLA* si fuera necesario.
- El prefijo de nivel siguiente, *NLA*, está destinado para numerar redes de los medianos y pequeños proveedores. El tamaño del campo *NLA* permite crear una jerarquía de dirección multinivel a través de la agregación de direcciones. Esta jerarquía reflejaría la del multinivel de los ISP.
- *SLA* está destinado a redes de direccionamiento de un suscriptor individual, tal como las subredes representan partes de la misma red corporativa. Se supone que el proveedor asigna para una compañía específica el número de subred que abarca un valor fijo de los

3 bits	13 bits	8 bits	24 bits	16 bits	64 bits
Prefijo de formato (FP)	Agregación del nivel superior (TLA)		Agregación del nivel siguiente (NLA)	Agregación del nivel de sitio (SLA)	ID de interfase

FIGURA 18.20 Estructura de una dirección única agregada global en un paquete IPv6.

campos *TLA* y *NLA*, los cuales en combinación representan una analogía del número de red en IPv4. La parte restante de la dirección (los campos de *SLA* y de *ID de interfase*) se encuentran a disposición del administrador. El administrador de la red de la compañía controla el proceso de formación de la dirección y no debe ponerse de acuerdo en este proceso con el proveedor. Al mismo tiempo, el campo de *ID de interfase* tiene un propósito específico: debe almacenar la dirección física del host. En este nivel, también es posible agregar direcciones de pequeñas subredes en subredes más grandes. El tamaño del campo *SLA* proporciona suficiente flexibilidad para construir una jerarquía de direcciones específica de la compañía.

- *La interfase ID* es un análogo del número de host en IPv4. La diferencia en IPv6 es que, por lo general, el identificador de la interfase sólo hace coincidir su dirección local (de hardware) en vez de representar un número de host asignado de modo arbitrario por un administrador. El identificador de interfase tiene una longitud de 64 bits, que permite situar ahí una dirección MAC (48 bits), una dirección X.25 (hasta 60 bits) y una dirección de nodo terminal ATM (48 bits), o un número de conexión virtual ATM (hasta 28 bits). En teoría, se espera poder utilizar direcciones locales de tecnologías emergentes. Tal como un enfoque de estilo IPX hace innecesario usar ARP, pues el procedimiento de mapear una dirección IP a una dirección local se convierte en trivial: se reduce a descartar simplemente la parte más significativa de la dirección. Además, en la mayoría de los casos, se elimina la necesidad de configurar en forma manual los nodos terminales. Esto se debe a que el host obtiene la parte menos significativa de la dirección, la ID de interfase, desde el hardware (adaptador de red, etc.) y el ruteador informa al nodo terminal acerca de la parte más significativa de la dirección: el número de red.

Como resulta evidente, al tener tal abundancia de redes en IPv6, la elaboración de subredes (o sea, utilizar máscaras para dividir redes en subredes) ya no tiene sentido. Por otra parte, un procedimiento inverso, la elaboración de superredes, tiene especial importancia. Los diseñadores de los estándares IPv6 consideran la agregación de dirección como el principal método del uso eficaz del espacio de dirección en la nueva versión de IP.

EJEMPLO

Supóngase que el cliente ha obtenido de un ISP un conjunto de direcciones IPv6, definidas por el prefijo siguiente: 20:0A:00:C9:74:05/48.

Analice este número. Como sus primeros 3 bits se han establecido a 001, ésta es una dirección única agregada global. Represente el prefijo 20:0A:00:C9:74:05/48 utilizando el formato estándar para este tipo de dirección (figura 18.21).

Esta dirección pertenece al proveedor de nivel superior, cuyas redes tiene el prefijo 20:0A/16. Este proveedor puede asignar algún intervalo de dirección con el prefijo común al proveedor de segundo nivel. Este prefijo común se creará con base en el prefijo del proveedor de nivel superior y en parte del campo NLA. La longitud del campo NLA asignado por el prefijo está determinada por la máscara que el proveedor de nivel superior debe especificar para el cliente: el proveedor de segundo nivel. Supóngase que en este ejemplo la máscara comprende 32 unos en los bits más significativos y que el prefijo resultante del proveedor de segundo nivel se asemeja al que sigue: 20:0A:00:C9/32.

De esta manera, el proveedor de segundo nivel tiene 16 bits del campo NLA para numerar las redes de sus clientes. La lista de clientes del proveedor de segundo nivel puede incluir proveedores de tercer nivel y más pequeños, aparte de suscriptores: compañías y organizaciones. Supóngase que el proveedor utilizó el siguiente byte del

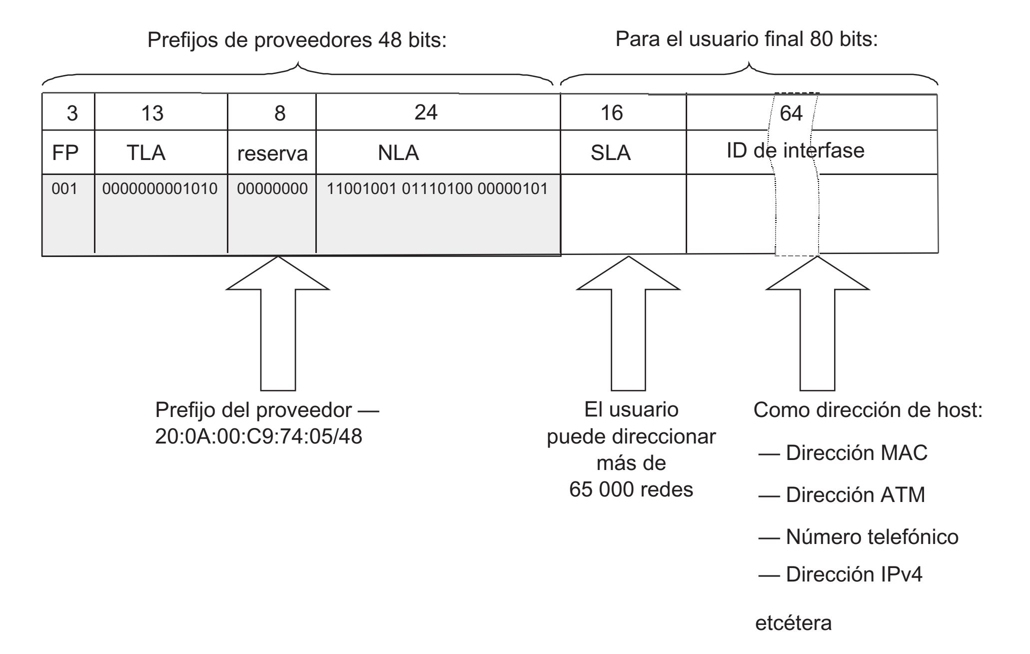


FIGURA 18.21 Ejemplo de una dirección única agregada global.

campo NLA (01110100) para pasar al proveedor de tercer nivel, el cual, a su vez, ha empleado el último byte del campo NLA para asignar un conjunto de direcciones para su cliente. De esta forma, la jerarquía de tres niveles de los proveedores ha formado el prefijo 20:0A:00:C9:74:05/48, que fue asignado al cliente.

IPv6 deja a disposición del cliente 2 bytes para numeración de redes (el campo *SLA*) y 8 bytes para numeración de hosts (el campo *ID de interfase*).

Al tener tan gran intervalo de números de subred, el administrador puede utilizarlo de diferentes maneras. Por ejemplo, puede seleccionar un direccionamiento directo de la red al asignar un valor específico del intervalo disponible de 65 535 direcciones sin utilizar las restantes. En redes grandes, una estructura jerárquica de redes basada en agregación de direcciones puede ser un método más eficaz para organizar el espacio de dirección, pues reduce el tamaño de las tablas de enrutamiento en ruteadores corporativos. En este caso, se utiliza la tecnología tradicional CIDR; no obstante, ésta es implementada por el administrador de la red de la compañía más que por el ISP.

Aparte de la dirección única agregada global considerada con anterioridad, existen otros tipos de direcciones unidirigidas:

- La *dirección de anillo* (*loopback*) 0:0:0:0:0:0:0:1 en IPv6 desempeña el mismo papel que la dirección 127.0.0.1 en IPv4.
- La *dirección indefinida* ::, que sólo comprende ceros, es una análoga de la dirección 0.0.0.0 en IPv4. Este valor indica que el host carece de una dirección IP asignada, la cual no debe aparecer en paquetes IP como una dirección de destino. Si aparece en el campo de la dirección fuente, esto significa que el paquete fue enviado antes que el host supiera su dirección IP (por ejemplo, antes de obtener una dirección desde el servidor DHCP).

Se supone que los segmentos de Internet que funcionan con base en IPv6 coexistirán con la otra parte de Internet que ha utilizado IPv4 durante mucho tiempo. Para asegurar que el host que soporta IPv6 puede utilizar la técnica de pasar paquetes IPv6 a través de la red IPv4

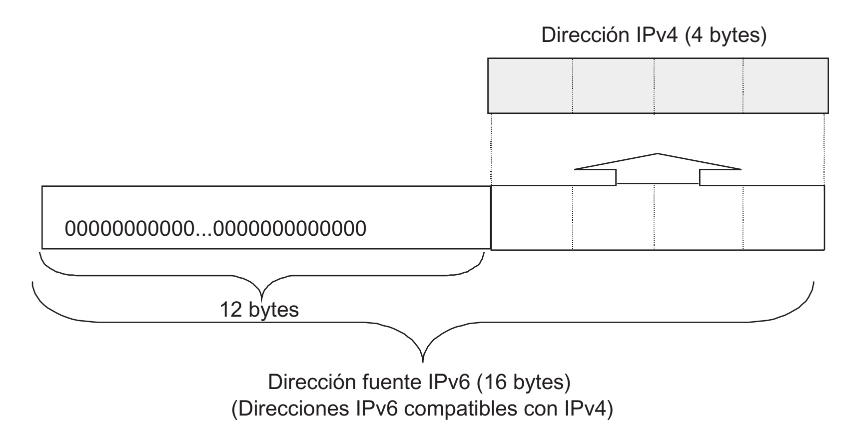


FIGURA 18.22 Conversión de IPv6 a IPv4.

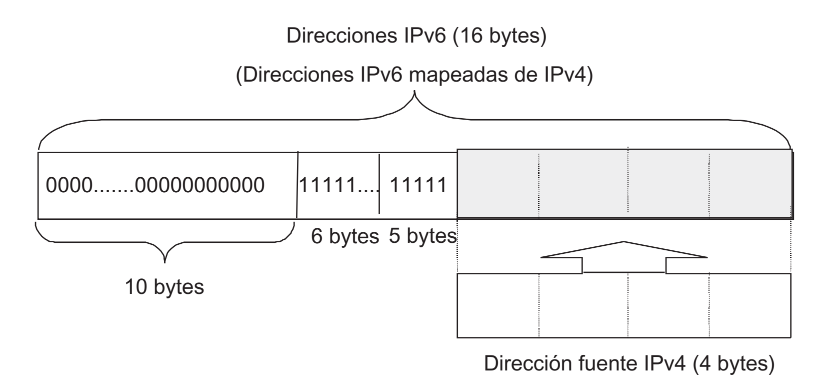


FIGURA 18.23 Conversión de IPv4 a IPv6.

de modo automático, se ha diseñado un subtipo especial de direcciones. Las direcciones de este subtipo llevan la dirección IPv4 en 4 bytes menos significativos de la dirección IPv6, mientras que 12 bytes más significativos de la dirección se llenan con ceros (figura 18.22). Este tipo de dirección unidirigida hace sencillo el procedimiento de convertir direcciones IPv6 a direcciones IPv4. Ambas se conocen como direcciones **IPv4 compatibles** con IPv6.

Existe una variante más de una dirección IPv6 que transporta una dirección IPv4: la dirección IPv4 mapeada a IPv6. Este tipo de dirección está destinada a resolver un problema inverso: pasar paquetes IPv4 a través de segmentos de Internet que funcionan de acuerdo con IPv6. Las direcciones de este tipo contienen una dirección IPv4 en cuatro bytes menos significativos, sus 10 bytes más significativos están llenos con ceros y el quinto y sexto bytes contienen unos, lo cual indica que el host soporta IPv4 (figura 18.23).

La investigación en el campo de la pormenorización de los subtipos de IPv6 está lejos de consumarse. Sólo 15% del espacio de dirección IPv6 tiene un propósito definido con claridad; la parte restante de las direcciones espera su turno para encontrar aplicaciones destinadas a resolver algunos de los numerosos problemas de Internet.

18.6.3 Formato de encabezado flexible

Uno de los objetivos más importantes para la modificación del formato del encabezado en IPv6 fue reducir el gasto general, o sea, disminuir la cantidad de información de control

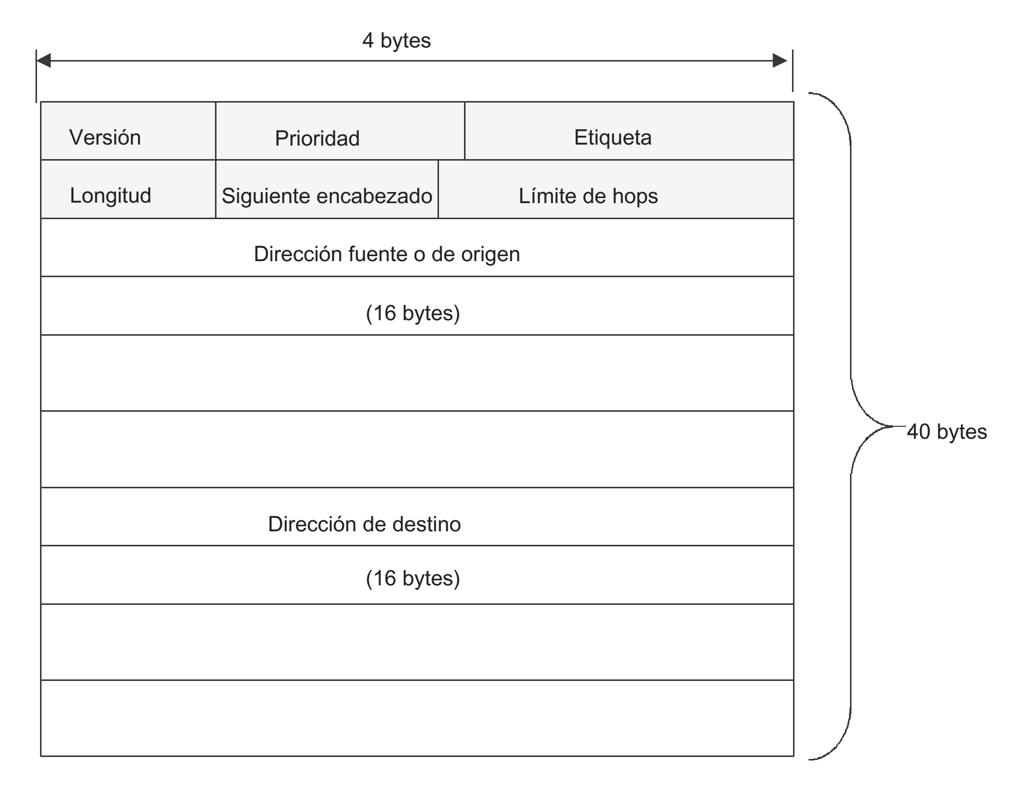


FIGURA 18.24 Formato del encabezado principal.

transmitida con cada paquete. Para este propósito, se introdujeron los conceptos de los encabezados *principal* y *adicional* en la nueva versión de IP. El encabezado principal siempre está presente, mientras que los **encabezados adicionales** son opcionales. Por ejemplo, los encabezados adicionales pueden contener información acerca de la fragmentación del paquete original, la ruta completa del paquete cuando se utiliza la técnica de enrutamiento de origen y la información requerida para proteger los datos que se transmiten.

El encabezado principal tiene la longitud fija de 40 bytes y su formato se muestra en la figura 18.24.

El campo de *encabezado siguiente* corresponde al campo de *protocolo* en IPv4 y define el tipo de encabezado que sigue al actual. Cada encabezado adicional siguiente contiene también el campo *encabezado siguiente*. Si un paquete IP no contiene encabezados adicionales, este campo deberá contener el valor asignado para protocolos tales como TCP, UDP, RIP, OSPF u otros definidos en el estándar IPv4.

En la actualidad, los tipos siguientes de encabezados adicionales se mencionan en propuestas del estándar IPv6:

- **Enrutamiento:** utilizado para especificar la ruta completa cuando se utiliza enrutamiento fuente o de origen.
- **Fragmentación:** contiene información relacionada con la fragmentación del paquete IP. Este campo es procesado en los nodos terminales.
- **Autenticación:** contiene información requerida para la auténtica sesión del nodo terminal y para asegurar la integridad del contenido de los paquetes IP.
- **Encapsulamiento:** contiene información requerida para asegurar la confidencialidad de los datos que se transmiten, al usar encriptación y desencriptación.

Encabezado principal IPv6

Encabezado del ruteador

Encabezado de fragmentación

Encabezado de autenticación

Encabezado de encapsulación

Opciones de destino

Paquete de protocolo de capa superior

FIGURA 18.25 Estructura del paquete IPv6.

- **Opción de salto en salto (Hop-by-Hop):** establece parámetros especiales utilizados cuando se procesan paquetes de acuerdo con el algoritmo de salto en salto.
- **Opciones de destino:** contiene información auxiliar para el nodo de destino.

De este modo, el formato del paquete IP puede tener un aspecto parecido al que se muestra en la figura 18.25.

Dado que para el enrutamiento del paquete sólo se requiere el encabezado principal (casi todos los encabezados adicionales se procesan sólo mediante los nodos terminales), esto reduce la carrera en los ruteadores. Por otra parte, la posibilidad de utilizar un gran número de parámetros adicionales *amplía la funcionalidad IP y la deja abierta para introducir nuevos mecanismos.*

18.6.4 Reducción de la carga en los ruteadores

Para mejorar el rendimiento de los ruteadores de Internet relacionados con su función principal, el envío de paquetes, IPv6 atiende las necesidades para que los ruteadores no tengan que realizar algunas labores subsidiarias:

- Trasladar las funciones de fragmentación de los ruteadores hacia los nodos terminales. En IPv6, los nodos terminales deben detectar el tamaño mínimo de la MTU a lo largo de la ruta que conecta el host fuente con el host de destino (esta técnica, conocida como *descubrimiento de la trayectoria MTU*, se utilizaba en IPv4). Los ruteadores IPv6 no llevan a cabo fragmentación de paquete. Por el contrario, solamente envían el mensaje ICMP

paquete demasiado extenso (packet too long) a los nodos terminales. Una vez que ha recibido un mensaje de esta clase, el host debe reducir el tamaño del paquete.

- Agregación de dirección, lo que reduce el tamaño de las tablas de dirección en los ruteadores. En consecuencia, disminuye el tiempo de búsqueda de la tabla y el tiempo requerido para actualizar las tablas. Al ocurrir todo esto, el tráfico auxiliar creado por los protocolos de enrutamiento también se reduce.
- Amplio uso de enrutamiento fuente o de origen en el que el nodo fuente especifica la ruta completa por la cual el paquete cruza por la red. Una técnica así evita que los ruteadores tengan que consultar la tabla de dirección cuando se selecciona el siguiente ruteador.
- Abandonar el procesamiento de parámetros opcionales del encabezado.
- Utilizar la dirección MAC del nodo como su número, lo que libera a los ruteadores de la necesidad de utilizar ARP.

La nueva versión de IP, un componente del proyecto IPv6, proporciona herramientas integradas de protección de datos. La implementación de las herramientas de protección en la capa de red las hará invisibles a las aplicaciones, porque entre la capa IP y la aplicación siempre habrá un protocolo de capa de transporte. Cuando se utiliza este enfoque, no será necesario volver a diseñar las aplicaciones. La nueva versión de IP con herramientas de seguridad integradas se conoce como IPSec. Las capacidades de este protocolo se examinarán con detalle en el capítulo 24.

La transición desde IPv4 hasta IPv6 apenas ha comenzado. Existen segmentos de Internet en los cuales los ruteadores soportan ambas versiones de IP. Estos fragmentos se conectan a otro mediante el uso de dicha red, con lo cual se forma el **6Bone**.

RESUMEN

- IP resuelve el problema de la entrega de datos entre los nodos de las interredes. Como es un protocolo de datagrama, no proporciona garantías para la confiabilidad de la entrega de los datos.
- Una característica de IP, a diferencia de otros protocolos de red (como IPX), es su capacidad para llevar a cabo fragmentación dinámica de los paquetes cuando se transmiten entre las redes que tienen diferentes valores de longitud máxima del campo de datos (MTU).
- La longitud máxima de un paquete IP es de 65 535 bytes. El encabezado por lo regular tiene una longitud de 20 bytes y contiene información acerca de las direcciones de red del emisor y el receptor, parámetros de fragmentación, TTL del paquete, suma de verificación y algunos otros datos.
- El formato de la tabla de enrutamiento IP depende de la implementación específica del ruteador. A pesar de las diferencias significativas en las formas de las tablas exhibidas en pantalla, todas ellas incluyen dos campos obligatorios, sin los cuales es imposible llevar a cabo el enrutamiento: *la dirección fuente o de origen* y la *dirección de destino*.
- Los registros se suministran a la tabla de enrutamiento desde las tres fuentes. En primer lugar, el software de la pila TCP/IP, como resultado de la configuración, conserva en esta tabla los registros acerca de las redes directamente conectadas y ruteadores predeterminados, además de los registros referentes a las direcciones de propósito especial. En segundo lugar, el administrador puede introducir de forma manual los registros relacionados con rutas específicas o con respecto al ruteador predeterminado. Finalmente, los protocolos

de enrutamiento registran de manera automática en su tabla los registros dinámicos acerca de las rutas existentes.

- Las máscaras proporcionan un método eficaz para estructurar las redes IP. Las máscaras dividen una red simple en varias subredes (elaboración de subredes) o agregan varias redes en una mayor (elaboración de superredes).
- La tecnología de enrutamiento en interdominio sin clases (CIDR) tiene un papel importante en el futuro de las redes IP. Esta tecnología resuelve dos problemas principales: asegurar el uso más eficaz del espacio de dirección disponible y reducir el número de los registros en las tablas de enrutamiento, pues un registro puede representar múltiples redes con un prefijo común.
- Desde principios de la década de 1990, la pila TCP/IP ha encontrado serios problemas que no podían ser resueltos sin modificar el formato del paquete IP y la lógica del procesamiento de los campos del encabezado IP. Como resultado, la comunidad de Internet decidió diseñar una versión nueva de IP, IPv6. Esta modernización tenía los objetivos siguientes: crear un sistema de direccionamiento escalable, mejorar el ancho de banda de la red a expensas de reducir el número de operaciones realizadas por los ruteadores, asegurar la calidad de los servicios de transporte y garantizar la seguridad de los datos transmitidos a través de la red.

PREGUNTAS DE REPASO

1. ¿Cómo se manifiesta la inestabilidad de IP?
2. Compare la tabla de dirección de un puente o un conmutador con la de un ruteador. Describa cómo se elaboran estas tablas. ¿Qué información contienen?, ¿de qué factores depende el tamaño de la tabla?
3. Considere un ruteador troncal de Internet. ¿Cuáles de los registros siguientes se encuentran en su tabla de enrutamiento en el campo *dirección de destino*?
   a) Números de todas las redes de Internet.
   b) Números de algunas redes de Internet (B).
   c) Números de algunas redes y direcciones completas de algunos hosts de Internet para los que están definidas rutas específicas.
   d) Direcciones de propósito especial, como 127.0.0.0 o 255.255.255.255 (D).
4. ¿Cuántos registros en rutas predeterminadas pueden incluirse dentro de la tabla de enrutamiento?
5. Proporcione ejemplos de ellos en situaciones en las cuales pueda surgir la necesidad de usar rutas específicas.
6. Cuando el enrutamiento está basado en máscaras, ¿contiene la máscara el paquete IP?
7. ¿Cuáles son las ventajas proporcionadas por tecnología CIDR?, ¿qué impide su uso extendido?
8. ¿Existe alguna relación entre la longitud del prefijo de un conjunto continuo de direcciones IP y el número de direcciones incluidas en ese conjunto?
9. ¿Por qué a menudo el registro de la ruta predeterminada contiene 0.0.0.0 con la máscara 0.0.0.0 como la dirección de la red de destino?
10. ¿Cuál de los elementos siguientes de la red puede llevar a cabo fragmentación?
    a) Solamente computadoras.
    b) Sólo ruteadores.
    c) Computadoras, ruteadores, puentes y conmutadores.
    d) Computadoras y ruteadores.

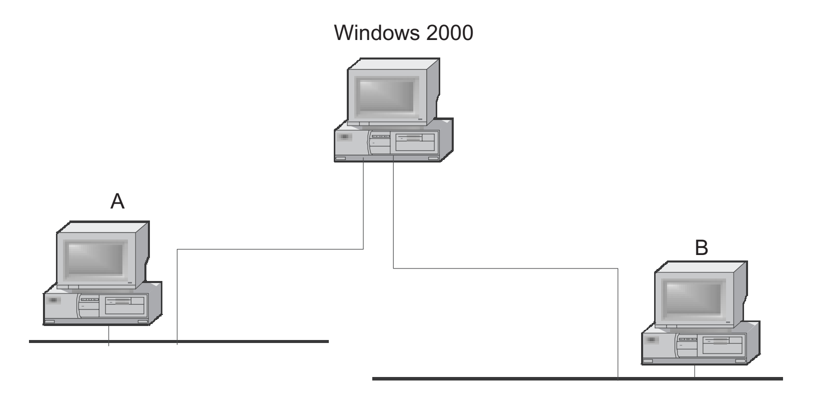


FIGURA 18.26 Dos segmentos de red conectados por una computadora.

11. ¿Qué ocurrirá al paquete si fue fragmentado en el transcurso de su transmisión y uno de los fragmentos no llega al host de destino después de terminar el tiempo de espera?
   a) La entidad IP del host emisor volverá a transmitir el fragmento perdido.
   b) La entidad IP del host emisor volverá a transmitir todo el paquete, el cual incluye el fragmento perdido.
   c) La entidad IP del host de destino descartará todos los fragmentos recibidos del paquete que contenía el fragmento perdido. La entidad IP del host emisor no tomará ninguna acción relacionada con la retransmisión de este paquete.

12. La figura 18.26 muestra una computadora con dos adaptadores de red a los cuales están conectados dos segmentos de red. Esta computadora ejecuta Windows 2000. ¿Puede la computadora A en un segmento intercambiar datos con la computadora B en otro segmento?

13. Estos segmentos utilizan diferentes protocolos de capa de enlace de datos, como de Internet y Token Ring. ¿Puede esto influir en la respuesta a la pregunta anterior?

14. ¿Cómo utiliza un administrador de IPv6 las máscaras?
   a) Las ignora debido a que no son necesarias.
   b) Utiliza elaboración de superredes.
   c) Usa elaboración de subredes.
   d) Emplea tanto la elaboración de superredes como la de subredes.

15. Si alguien establece que una transmisión es un caso particular de multidifusión, ¿será correcta esta afirmación?, ¿será correcto establecer que una transmisión es un caso particular de difusión enviada a cualquier nodo?

16. ¿Es posible para la misma interfase de red tener de manera simultánea varias direcciones IPv6 de tipos distintos: unidirigida, enviada a cualquier modo y multidirigida?

PROBLEMAS

1. La sección "Traslape de espacios de dirección" de este capítulo contenía el ejemplo de planeación de red. En este ejemplo, un administrador de red ha formulado los requisitos siguientes: 600 direcciones para Ethernet, 200 direcciones para la red Token Ring, 10 direcciones para DMZ y 4 direcciones para red de conexión. Resuelva el mismo problema para el caso en el que están planeadas 300 estaciones de trabajo para la red Token Ring.

- ¿Qué conjunto de direcciones debe ser recibido desde el ISP? En este ejemplo, el ISP proporcionará al cliente un conjunto de dirección continuo.
- ¿Cómo debería distribuir el administrador estas direcciones entre cuatro redes?
- ¿Cómo se verían las tablas de enrutamiento de los ruteadores R1 y R2?

19

PROTOCOLOS PRINCIPALES DE LA PILA TCP/IP

DESCRIPCIÓN DEL CAPÍTULO

19.1 INTRODUCCIÓN

Primero se estudiarán TCP y UDP, como protocolos que desempeñan el papel de intermediarios entre los programas de aplicación y la infraestructura de transporte de la red. Aunque el objetivo principal de la capa de Internet, con la que se relaciona el protocolo de Internet (IP), es transmitir datos entre interfases de red utilizando la interred, la tarea más importante de la capa de transporte, llevada a cabo por protocolos como el de control de transmisión (TCP) y el de datagrama del usuario (UDP), consiste en transmitir datos entre los *procesos de aplicación* que se ejecutan en computadoras conectadas a la red.

Entonces, se analizarán los protocolos de enrutamiento destinados a la construcción automática de tablas de ruteo, utilizados como la base para el envío de paquetes de capa de red. En contraste con los protocolos de red, como IP o IPX, los de enrutamiento son opcionales, debido a que una tabla de ruteo puede crearse de forma manual por el administrador de la red. Sin embargo, en redes grandes con topología compleja y muchas rutas alternativas, los protocolos de enrutamiento realizan la importante tarea de automatizar la construcción de las tablas de ruteo. También pueden encontrar nuevas rutas en casos de cambios en la estructura de la red, incluidas fallas o los casos en que se introducen nuevos ruteadores o enlaces de comunicaciones.

También se estudiará el protocolo de mensajes de control de Internet (ICMP), la herramienta para informar al emisor o remitente acerca de las razones por las cuales sus paquetes no fueron entregados al destino. Del diagnóstico, ICMP se utiliza para *monitoreo de la red.* Por ejemplo, los mensajes ICMP se usan como el fundamento para herramientas de monitoreo conocidas en la red IP tales como ping y traceroute.

19.2 PROTOCOLOS DE CAPA DE TRANSPORTE TCP Y UDP

PALABRAS CLAVE: protocolo de control de transmisión (TCP, Transmisión Control Protocol), protocolo de datagrama del usuario (UDP), puerto, socket o enchufe, multiplexaje, demultiplexaje, números de puerto estándar, puerto bien conocido, puerto dinámico, puerto UDP, puerto TCP, mejor esfuerzo, paquete UDP, datagrama del usuario, puerto de origen, puerto de destino, número de secuencia, número de reconocimiento, bits de código, datos urgentes, ventana, suma de verificación, apuntador urgente, opciones, amortiguamiento, conexiones lógicas, segmento, algoritmo de ventana deslizante y tiempo de viaje redondo (RTT, Round Trip Time).

Como ya se mencionó, la tarea principal de la capa de transporte se realiza mediante el protocolo de control de transmisión (TCP), definido en RFC 793, y el protocolo de datagrama de usuario (UDP), descrito en RFC 768. Esta tarea consta de transmisión de datos entre los procesos de aplicación que se ejecutan en computadoras conectadas a la red. Dado que TCP y UDP se relacionan con la misma capa, tienen mucho en común. Ambos protocolos aseguran la interfase a los protocolos de aplicación de capa superior mediante la transmisión de los datos que llegan al host hacia las aplicaciones apropiadas. Al mismo tiempo, dichos protocolos utilizan los conceptos de **puerto** y **socket** y soportan la interfase a la capa IP de red subyacente al encapsular sus PDU en paquetes IP. De manera semejante a los protocolos de la capa de aplicación, las entidades de protocolo tanto de TCP como de UDP se instalan sólo en los nodos terminales. Sin embargo, como se verá posteriormente, las diferencias entre TCP y UDP son más numerosas que sus similitudes.

19.2.1 Puertos

Cada computadora puede ejecutar varios procesos; además, cada proceso de aplicación puede tener varios puntos de acceso que sirvan como direcciones de destino para paquetes de datos. Por lo tanto, después que el paquete es entregado a la interfase de red del host de destino mediante IP, es necesario pasar estos datos al proceso específico al que se hallan destinados estos datos.

También puede llevarse a cabo la tarea inversa: los paquetes enviados hacia la red por aplicaciones diferentes que se ejecutan en el mismo nodo terminal se procesan mediante el mismo IP. En consecuencia, la pila de protocolos debe proporcionar un medio para "recolectar" los paquetes desde diferentes aplicaciones y pasarlos a IP. Tanto TCP como UDP pueden realizar este trabajo.

El procedimiento realizado por TCP/UDP para recibir los datos que llegan desde varios servicios de aplicación se denomina **multiplexaje**. Un procedimiento inverso, empleado por TCP/UDP para distribuir los paquetes que llegan desde la capa de red entre el conjunto de servicios de capa superior, se conoce como **demultiplexaje** (figura 19.1).

Para cada puerto de aplicación, TCP y UDP soportan dos colas: la de paquetes que llegan a esta aplicación desde la red y la de paquetes enviados por la aplicación hacia la red. Los paquetes que llegan hacia la capa de transporte son organizados por el sistema operativo como conjuntos de colas hacia varios puntos de acceso de diversos procesos de aplicación. En la terminología TCP/IP, tales colas de sistema se llaman *puertos*. (No hay que confundir los puertos de aplicación con los puertos de hardware, es decir, las interfases de red, el equipo de red.) Obsérvese que tanto las colas de entrada como de salida de la misma aplicación se consideran el mismo puerto. Para la identificación única y sin ambigüedades de los puertos, se les asignan números de puerto, los cuales se utilizan para aplicaciones de direccionamiento.

Existen dos métodos para asignar números de puerto a las aplicaciones: el *centralizado* y el *local*. Cada uno de estos métodos tiene su intervalo de números de puerto: para el método centralizado, se asignan los números de puerto desde el 0 hasta el 1 023, mientras que el método local usa los números de puerto que van desde el 1 024 hasta el 65 535.

Si los procesos son servicios públicos populares, como el protocolo de transferencia de archivos (FTP), telnet, http, TFTP o DNS, se les asignan **números de puerto estándares**,

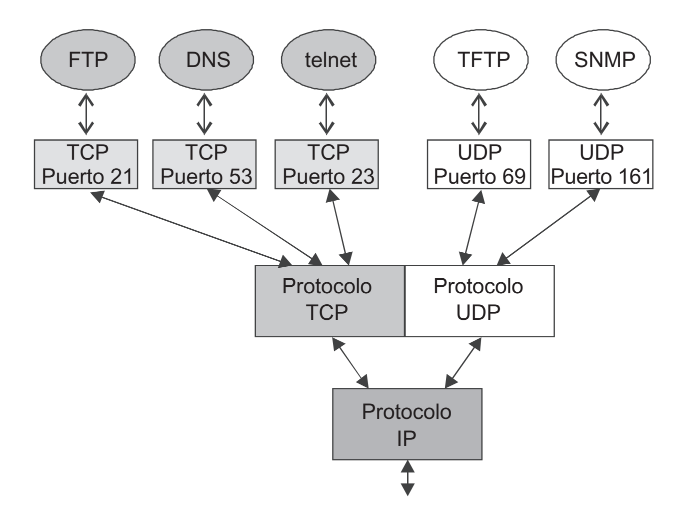


FIGURA 19.1 Multiplexaje y demultiplexaje en la capa de transporte.

también denominados **números de puertos bien conocidos**. Estos números son estándares de Internet designados (RFC 1700 y RFC 3232). Por ejemplo, el número 21 está asignado al servicio FTP, mientras que el 23 está asignado al servicio de telnet. Las direcciones asignadas son únicas, lo cual significa que no puede emplearlas ninguna otra aplicación.

Para aplicaciones que no se utilizan mucho y son muy conocidas, los diseñadores de aplicaciones o el sistema operativo asignan números en respuesta a la solicitud de la aplicación. En cada computadora, el sistema operativo soporta la lista de números de puerto asignados y disponibles. Cuando llega una solicitud desde alguna aplicación y se ejecuta en una computadora local, el sistema operativo asigna al primer número de puerto disponible. Tales números se conocen como dinámicos. Posteriormente, todas las aplicaciones de la red tendrán acceso a esta aplicación al utilizar el número de puerto asignado a ella. Después que se hace la aplicación terminal, el número de puerto local asignado a ésta es devuelto a la lista de números de puerto disponibles y puede asignarse a otra aplicación. Los **números de puerto dinámico** son *únicos dentro de los límites de cada computadora*; no obstante, la situación en la cual aplicaciones que se ejecutan en diferentes computadoras tengan números de puerto coincidentes es bastante común. Como regla, las partes del cliente de las aplicaciones bien conocidas (DNS, WWW, FTP, telnet, y así sucesivamente) reciben números de puerto dinámicos desde el sistema operativo.

Toda esta información que relacionan los puertos se aplica de igual forma a ambos protocolos de capa de transporte. Principalmente, no hay dependencia entre asignar números de puerto para aplicaciones mediante el uso de TCP y el mismo procedimiento para las aplicaciones que trabajan con UDP. Las aplicaciones que pasan datos a la capa IP por medio de UDP tienen los números conocidos como **puertos UDP**. De forma similar, a las aplicaciones que emplean TCP se les asignan **puertos TCP**.

En ambos casos, pueden ser números de puertos asignados y dinámicos. Los intervalos de donde se asignan los puertos TCP y UDP coinciden: los números desde el 0 hasta el 1 023 son para números de puerto asignados, mientras que los números desde el 1 024 hasta el 65 535 son para números de puerto dinámicos. Sin embargo, no hay relación entre los números de puerto TCP y UDP asignados. Incluso si coinciden los números de puerto TCP y UDP, identifican diferentes aplicaciones. Por ejemplo, a una aplicación se le puede asignar el puerto TCP 1750, mientras que otra puede utilizar el puerto UDP 1750. Cuando una aplicación puede elegir entre TCP y UDP (un ejemplo de tal aplicación es DNS), se asigna un número de puerto coincidente TCP y UDP conveniente para memorizar. Por ejemplo, DNS puede emplear el puerto TCP 53 o el puerto UDP 53.

19.2.2 UDP

UDP es un protocolo de datagrama (es decir, el protocolo que funciona de acuerdo con el principio del **mejor esfuerzo** sin establecer una colección lógica). Dado que es un protocolo de datagrama, un UDP no garantiza la entrega de sus mensajes y, en consecuencia, no compensa la insuficiente confiabilidad de IP, que también es un protocolo de datagrama.

La unidad de datos de UDP se conoce como **paquete UDP** o **datagrama de usuario**. Cada paquete UDP transporta un *mensaje de usuario por separado* (figura 19.2). Esto produce una limitación natural: un datagrama UDP no puede exceder la longitud del campo de datos IP que, a su vez, está limitado por el tamaño de la trama de la tecnología de la red subyacente. Por lo tanto, si se desborda el búfer de UDP, se descartarán los datos de la aplicación. El encabezado UDP abarca cuatro campos de 2 bytes, que contienen los números de puerto del emisor y el receptor, la suma de verificación y la longitud del datagrama.

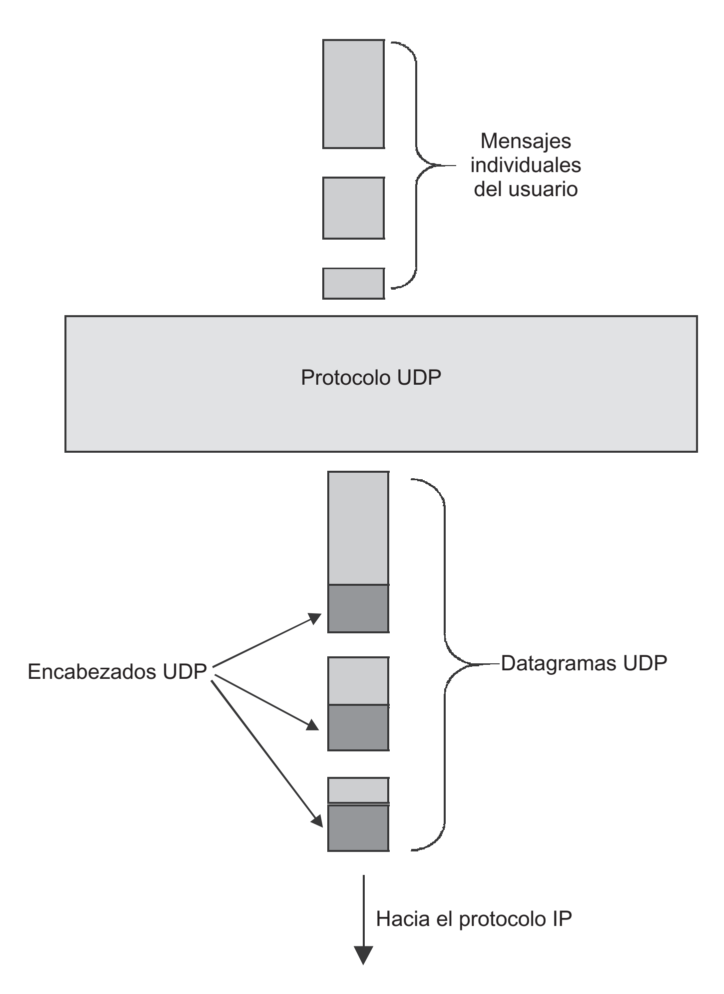


FIGURA 19.2 Formación del datagrama UDP.

Aquí se proporciona un fragmento del encabezado UDP con los campos llenos:

```
Source Port = 0x0035
    Destination Port = 0x0411
    Total length = 132 (0x84) bytes
    Checksum = 0x5333
```

En este datagrama UDP, el campo de datos, como se sigue del encabezado, tiene una longitud de 132 – 8 bytes y contiene mensaje desde el servidor que en ese punto puede ser detectado por el número de puerto del origen, `Source Port = 0x0035`, el cual corresponde al número de puerto estándar de servidor DNS, 53.

A juzgar por la simplicidad del encabezado, UDP no es un protocolo complicado. Las funciones se reducen a multiplexar y demultiplexar datos entre la red y las capas de aplicación. Considérese cómo resuelve UDP el problema del multiplexaje. El uso de números de puerto parece ser una forma natural de llevar a cabo esta tarea. Las tramas que conducen los datagramas UDP llegan a la interfase de red del host, donde los protocolos de cada pila las procesan secuencialmente y por último se pasan a UDP. El UDP recupera el número de puerto de destino del encabezado del paquete y los datos pasan al puerto apropiado de la aplicación correspondiente (es decir, realiza la tarea del demultiplexaje.

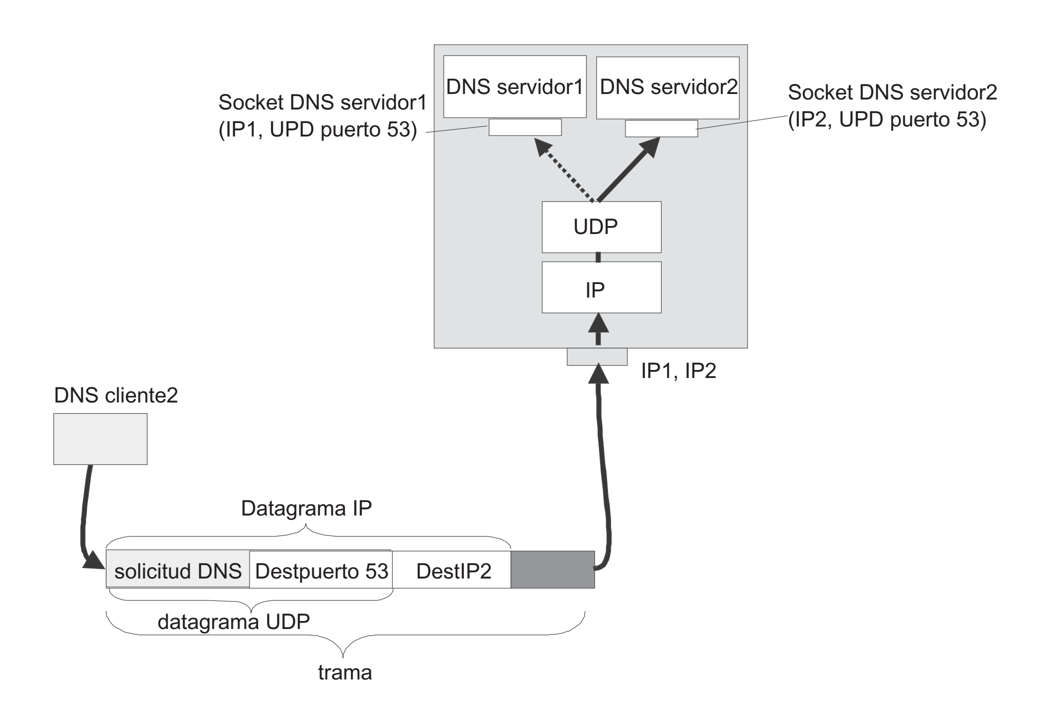


FIGURA 19.3 Demultiplexaje UDP basado en sockets.

Esta solución parece lógica y simple; sin embargo, en la práctica no funciona si *se ejecutan varias copias de la misma aplicación* en el mismo nodo terminal. Supóngase que dos servidores de DNS corren en el mismo host y que ambos utilizan UDP para pasar sus mensajes (figura 19.3). Al servidor DNS le ha sido asignado un puerto UDP bien conocido: 53. Al mismo tiempo, cada servidor que en ese puerto puede dar servicio a sus clientes tiene sus propias bases de datos y personalizadas configuraciones individuales. Cuando llega una solicitud desde un cliente de DNS a la interfase de red de esta computadora, el datagrama UDP especificará el número de puerto 53, que se relacionaría igualmente con ambos servidores DNS. ¿A cuál de estos servidores debe pasar el UDP de la consulta? Para eliminar esta ambigüedad, se ha utilizado el enfoque siguiente: copias distintas de las mismas aplicaciones instaladas en la misma computadora tienen asignadas diferentes direcciones de IP. En este ejemplo, el servidor1 DNS tiene la dirección IP1, mientras que el servidor2 en ese puerto tiene asignada la dirección IP2.

De este modo, la dirección del proceso de aplicación dentro de una red (e incluso dentro de una computadora) está definida sin ambigüedades mediante el par compuesto por la *dirección IP* y el número de *puerto UDP*. Este par se denomina **socket UDP**. El uso de sockets permite que el UDP haga el demultiplexaje correctamente.

NOTA *En esta relación cabe aclarar el patrón simplificado de acuerdo con el cual el paquete viaja hasta la pila de protocolo. Como se ha mencionado en capítulos anteriores, después de que el paquete que llega desde la red es procesado por IP, se descarta el encabezado de este paquete y únicamente se pasa el contenido del campo de datos del paquete, por ejemplo: éste puede ser el datagrama UDP. Sin embargo, cuando se explicó este mecanismo, se omitió un detalle importante: con el contenido del campo*

de datos, la dirección IP de destino recuperada del encabezado del paquete se pasa a la capa de transporte. *El UDP recupera el número de puerto desde el encabezado del datagrama UDP y, con base en el socket (*dirección IP de destino y número de puerto de destino*) se lleva a cabo el **demultiplexaje**.*

19.2.3 Formato de segmento TCP

La información suministrada a TCP desde los protocolos de capa superior es considerada por TCP un **flujo de bytes no estructurado**. Los datos entrantes se almacenan temporalmente en búfer por TCP. Entonces el protocolo "recorta" algunos segmentos de datos continuos,[1] los suministra con el encabezado y los pasa a la capa de red (figura 19.4).

El encabezado del segmento TCP contiene muchos más campos que el encabezado UDP, debido a las capacidades más avanzadas de TCP, a saber:

- **Puerto fuente:** este campo toma 2 bytes e identifica el proceso del emisor o remitente.
- **Puerto destino:** este campo toma 2 bytes e identifica el proceso de destino.
- **Número de secuencia:** este campo toma 4 bytes y especifica el número del byte que define el desplazamiento (offset) del segmento en relación con el flujo de los datos que se envían (es decir, el número del primer byte en este segmento).
- **Número de reconocimiento:** este campo es de 4 bytes y contiene el número del máximo byte en el segmento recibido incrementado en uno. Este valor es el utilizado como reconocimiento. Si el bit de verificación *ACK* está habilitado, este campo contendrá el número de cola siguiente que el emisor de este datagrama esperaría recibir como acuse de recibo o señal de reconocimiento.

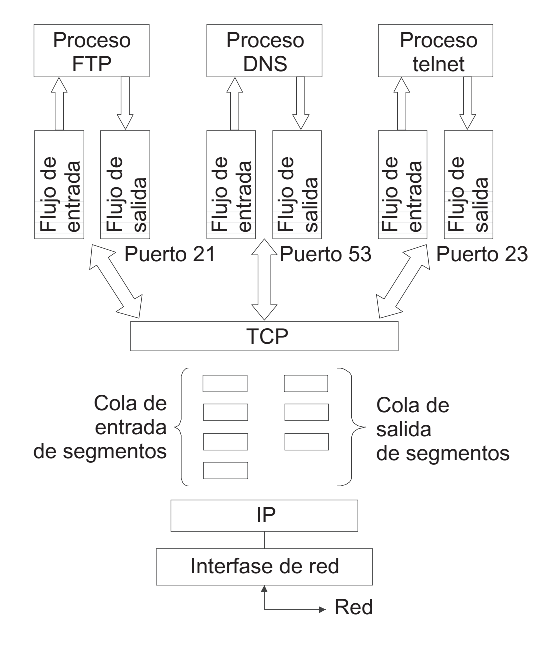


FIGURA 19.4 Formación de segmentos TCP de un flujo no estructurado de bytes.

[1] Nótese que el término *segmento* se usa tanto para designar la unidad de transmisión de datos como un todo (el campo de datos y el encabezado TCP) y sólo el campo de datos.

- **Longitud de encabezado (Hlen):** este campo de 4 bytes especifica la longitud del encabezado del segmento TCP, medido en palabras de 32 bits. La longitud del encabezado no es fija y puede variar, lo cual depende de los parámetros establecidos en el campo de *Opciones*.
- **Reservado:** este campo reservado tiene 6 bits y está reservado para uso futuro.
- **Bits de codificación:** este campo tiene seis bits que contienen información auxiliar acerca del tipo de este segmento. Dicha información se especifica al establecer a uno los siguientes bits de este campo:
  - **Datos urgentes:** son un mensaje urgente.
  - **ACK:** admite el segmento recibido.
  - **PSH:** solicita que se envíe el mensaje sin esperar a que se llene el búfer. Observe que TCP puede esperar hasta que el búfer se encuentre lleno antes de enviar el segmento. Si se necesita transmisión inmediata, la aplicación deberá informar al protocolo mediante el uso de este parámetro "push" (de empilamiento).
  - **RST:** solicita la restauración de la conexión.
  - **SYN:** este mensaje se utiliza para sincronizar los contadores de datos transmitidos cuando se establece una conexión.
  - **FIN:** es el atributo que especifica que el extremo que transmite ha enviado el último byte en el flujo de datos transmitidos.
- **Ventana:** este campo de 2 bytes especifica el número de bytes de datos, a partir del byte cuyo número se especifica en el campo de reconocimiento, cuya llegada es esperada por el emisor del segmento actual.
- **Suma de verificación (checksum):** este campo de 2 bytes contiene la suma de verificación.
- **Apuntador urgente:** este campo ocupa 2 bytes, se utiliza con el bit de código *URG* y especifica el final de los datos que deben recibirse urgentemente a pesar del desbordamiento del búfer. También, si se han de enviar algunos datos a la aplicación de destino fuera de turno, la aplicación del emisor debe informar del TCP mediante el uso del parámetro *URGENT DATA* (DATOS URGENTES).
- **Opciones:** este campo tiene longitud variable y puede ser ignorado. La longitud máxima de este campo es de 3 bytes. El campo se utiliza para resolver tareas auxiliares, por ejemplo: la selección de la longitud de segmento máximo. Las opciones pueden localizarse al final del encabezado TCP y su longitud debe ser un múltiplo de 8 bits.
- **Relleno:** este campo puede tener longitud variable. Es un campo ficticio utilizado para complementar el encabezado de tal modo que su tamaño sea igual a un número entero de palabras de 32 bits.

19.2.4 Conexiones lógicas como base para la confiabilidad de TCP

La diferencia principal entre TCP y UDP es que el primero tiene que llevar a cabo una tarea adicional. Esta tarea consiste en asegurar la *entrega confiable* de los mensajes a través de la interred, cuya totalidad de nodos usa el no confiable protocolo de datagrama IP para la transmisión de mensajes.

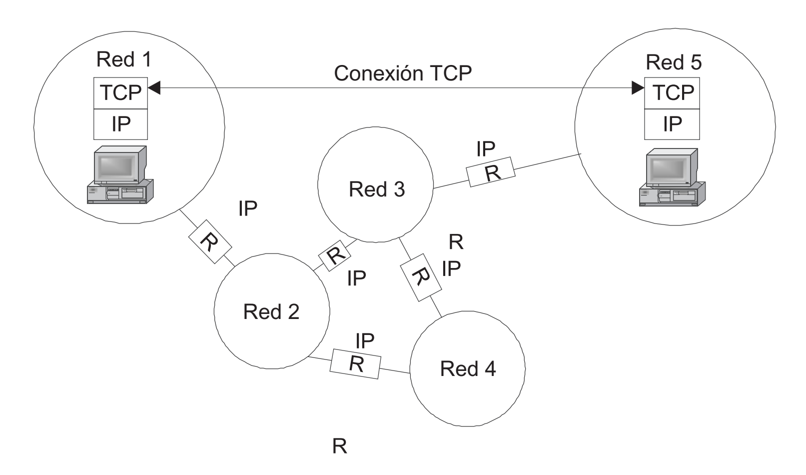


FIGURA 19.5 La conexión TCP crea un canal de comunicaciones confiable entre nodos terminales.

La figura 19.5 muestra redes conectadas por ruteadores, donde están instaladas entidades IP. Las entidades TCP instaladas en nodos terminales resuelven el problema de asegurar la *entrega confiable* de los datos al establecer **conexiones lógicas**[2] entre sí. TCP asegura que los elementos transmitidos no se pierdan, dupliquen o lleguen al receptor fuera de lugar.

- Cuando se establece una conexión lógica, las entidades TCP negocian los parámetros de procedimiento de intercambio de datos. En TCP, cada parte envía los parámetros siguientes a su asociado: el *tamaño máximo de segmentos* que está listo para recibir.
- El *máximo volumen de datos* (posiblemente de diversos segmentos) permite que otra parte transmita en su dirección, incluso si esa parte todavía no ha recibido un acuse de recibo para la anterior porción de datos (este parámetro se conoce como **tamaño de ventana**).
- El *número de inicio del byte* desde el que comienza el conteo del flujo de datos funciona dentro del marco de la conexión actual.

Como resultado de este proceso de negociación entre las entidades TCP de ambas partes, se definen los parámetros de conexión. Algunos parámetros permanecen constantes en toda la sesión; otros parámetros pueden modificarse de manera adaptativa. Por ejemplo, el tamaño de ventana de la parte emisora cambia dinámicamente, lo cual depende de la carga del búfer de la parte receptora y de la confiabilidad global de la operación de la red. La creación de la conexión también significa que el sistema operativo en cada computadora asigne recursos específicos del sistema para organizar los búferes, temporizadores y contadores. Estos recursos se asignarán a la conexión desde su creación y hasta la terminación de aquélla.

La conexión TCP lógica se identifica de manera unívoca mediante un *par de sockets*.

Cada enchufe puede participar de manera simultánea en varias conexiones. Por ejemplo, supóngase que existen tres enchufes de tres aplicaciones: (IP_1, n_1), (IP_2, n_2) e (IP_3, n_3). IP_1,

[2] Véase la sección “Conexión lógica” en el capítulo 3.

IP_2 e IP_3 son direcciones IP, mientras que n_1, n_2 y n_3 son sus números de puerto TCP. En este caso, es posible crear las conexiones siguientes:

Conexión 1: $\{(IP_2, n_2), (IP_1, n_1)\}$
Conexión 2: $\{(IP_1, n_1), (IP_3, n_3)\}$
Conexión 3: $\{(IP_2, n_2), (IP_3, n_3)\}$

La figura 19.6 muestra las conexiones 1 y 3 creadas por el enchufe (IP_2, n_2).

Ahora se explicará cómo TCP realiza la tarea de demultiplexaje. Considere el ejemplo siguiente: suponga que algún ISP proporciona servicio de hosting de web, lo cual significa que los clientes pueden instalar sus servidores web en el servidor perteneciente a este ISP. El servidor web está basado en el protocolo de capa de aplicación HTTP, que a su vez utiliza TCP, el cual espera por las consultas de los clientes web (navegadores) que exploran el puerto bien conocido 80.

La figura 19.7 muestra la variante de hosting con dos servidores web: **www1.model.com**, con la dirección IP, IP_1 y **www2.tour.com**, con la dirección IP_2. Cada servidor puede dar servicio a varios clientes al mismo tiempo, quienes pueden trabajar de manera simultánea con WWW1 y WWW2. El trabajo de cada cliente requiere que el servidor guarde de manera constante los números de las páginas leídas, los parámetros de la sesión y así sucesivamente, esto es, crear una conexión lógica individual. Una conexión así es creada por TCP para cada par cliente-servidor. Cada conexión se identifica de manera unívoca mediante un par de sockets correspondientes.

La figura 19.7 muestra dos navegadores con los sockets (IP_k, n_k) e (IP_m, n_m). El usuario del navegador *k* tiene acceso de modo simultáneo a los servidores WWW1 y WWW2. La presencia de conexiones individuales para trabajar con cada uno de estos dos servidores garantiza la separación de los flujos de información. El usuario nunca tendrá que preguntar cuál servidor ha enviado cuál página a él. De manera simultánea con el usuario del navegador *k*, el usuario del navegador *m* tiene acceso al servidor WWW2. En este caso, ambos usuarios trabajan dentro del marco de conexiones lógicas individuales, las cuales aíslan los flujos de

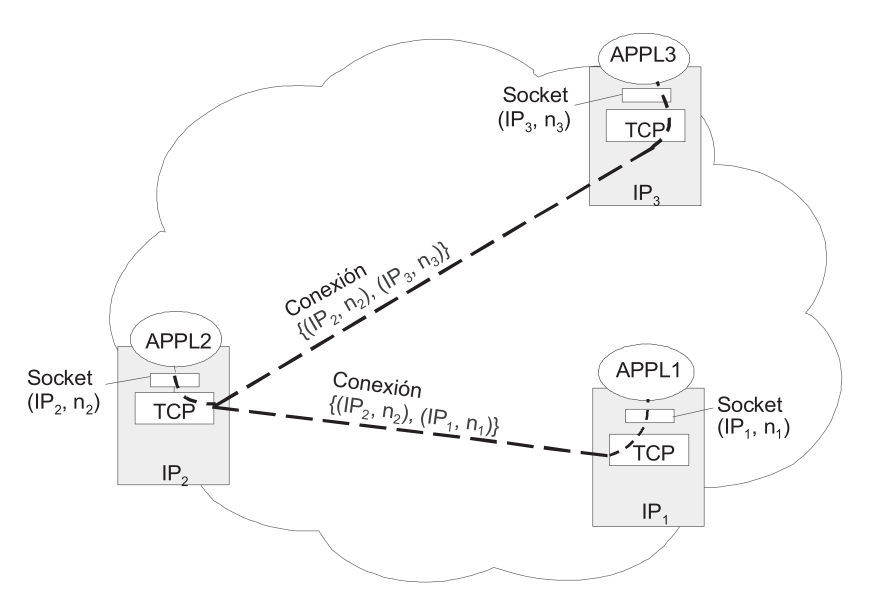


FIGURA 19.6 Un socket puede participar en varias conexiones.

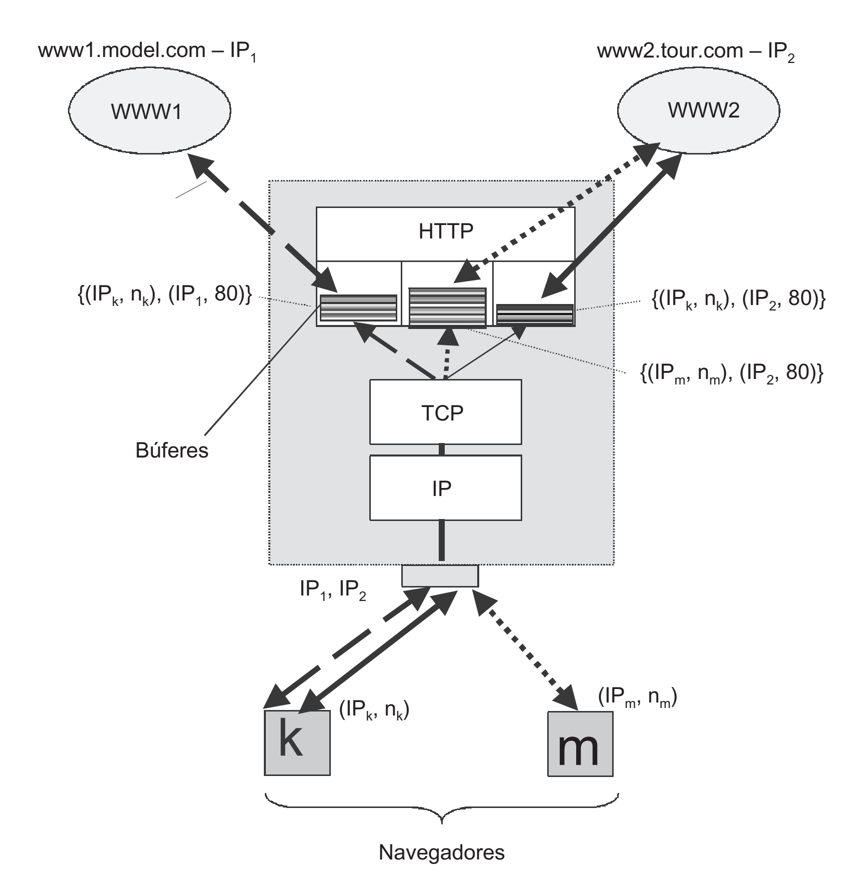


FIGURA 19.7 Demultiplexaje basado en una conexión TCP.

información de dichos usuarios. La figura 19.7 muestra varios búferes, cuyo número está definido por la cantidad de conexiones lógicas más que por el número de servidores web o la cantidad de clientes. Los mensajes se envían a estos búferes según los valores de los enchufes del emisor y el receptor.

Así, *TCP lleva a cabo el demultiplexaje con base en las conexiones lógicas.*

19.2.5 Número de secuencia y número de reconocimiento

En TCP, debe reconocerse la transmisión correcta de cada segmento dentro del marco de la conexión establecida. Los *reconocimientos* (o *acuses de recibo*) son un método tradicional para asegurar comunicaciones confiables. El TCP utiliza un mecanismo de reconocimiento particular: el **algoritmo de ventana deslizante**.[3]

[3] Para más detalles, véase la sección "Retransmisión de datos y la ventana deslizante" en el capítulo 6.

El algoritmo de ventana deslizante implementado en TCP tiene una característica específica: aunque la unidad de datos transmitidos es un *segmento*, la ventana se define como el conjunto de *bytes* numerados o el flujo de datos no estructurado que llega desde la capa superior y es almacenado temporalmente en un búfer por TCP.

Cuando se establece una conexión, ambas partes negocian el número de inicio del byte desde el cual se llevará a cabo el conteo para la duración de la conexión. Cada parte tiene su propio número inicial. El identificador de cada segmento es el número de su primer byte. Los bytes dentro de los límites de un segmento se numeran de tal manera que el primer byte de datos que sigue inmediatamente al encabezado tiene el número más pequeño, mientras que los bytes que siguen tienen números crecientes de modo secuencial (figura 19.8).

Cuando el remitente envía un segmento TCP, coloca el número de su primer byte en el campo del *número de secuencia* (*Sequence Number*) del encabezado. De este modo, la figura 19.9 muestra que los números siguientes sirven como identificador del segmento: 32 600, 34 060, 35 520, etc. Con base en estos números, la entidad TCP del receptor distingue el segmento específico de los otros y coloca el fragmento recibido dentro del flujo común de bytes. Aparte de esto, es capaz de determinar si dicho segmento es un duplicado o el recibido con anterioridad, si algunos datos se pierden entre dos segmentos recibidos, etcétera.

El receptor del segmento envía un acuse de recibo o reconocimiento en respuesta. Este reconocimiento es un segmento en el cual el receptor coloca el número que excede el número máximo de byte en el segmento recibido por uno. Este número se denomina *número de reconocimiento* (*Acknowledge Number*). Para los segmentos que contiene la figura 19.9, el número del último byte de cada segmento incrementado por uno sirve como un reconocimiento de recepción (un número de reconocimiento). Para el primer segmento enviado, éste será el número 34 060; para el segundo segmento, éste será el número 35 520, y así sucesivamente.

El número de reconocimiento suele interpretarse como el número del siguiente byte de datos esperado. En TCP, el reconocimiento se envía sólo después de la recepción de datos

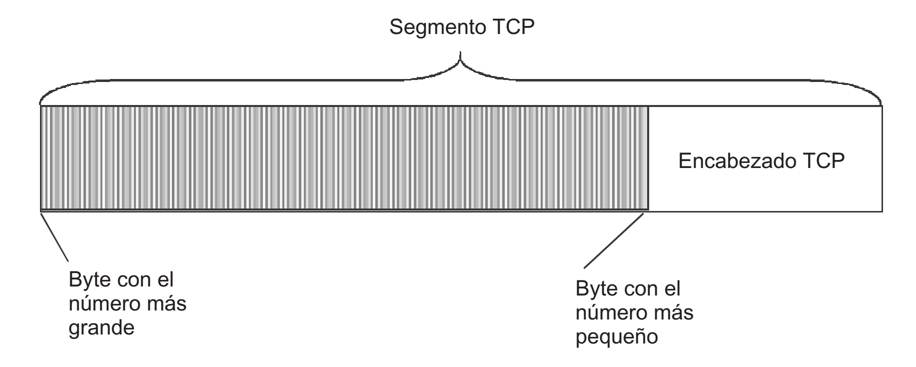


FIGURA 19.8 Numeración de bytes dentro de un segmento TCP.

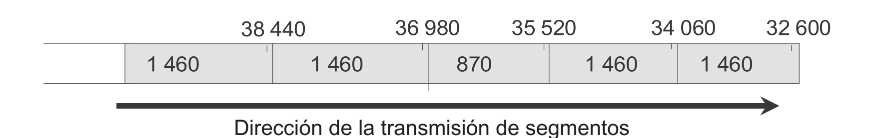


FIGURA 19.9 Número de secuencia y número de reconocimiento.

correcta, pero no se envían reconocimientos negativos. De esta manera, la ausencia de un reconocimiento significa que el segmento fue perdido, que el receptor recibió un segmento corrompido o que el reconocimiento se perdió.

En el protocolo, el mismo segmento puede contener tanto los datos que la aplicación envía a la otra parte como el reconocimiento en el cual la entidad TCP reconoce la recepción de los datos.

19.2.6 Ventana del receptor

TCP es un protocolo dúplex, lo cual significa que el procedimiento de intercambio de datos bidireccional es regulado dentro del marco de una conexión simple. Cada parte actúa de manera simultánea como emisor y como receptor y cada una tiene un par de búferes: uno es para almacenar los segmentos recibidos, mientras que el otro se destina a los segmentos que esperan a ser enviados. Aparte de esto, existe un búfer para almacenar copias de los segmentos enviados, cuyos reconocimientos o acuses de recibo todavía no han llegado (figura 19.10).

En el proceso de establecer una conexión y más adelante durante la transmisión bidireccional, ambas partes, que actúan como receptores, se envían entre sí las denominadas **ventanas de receptor**. *Cada una de las partes, una vez que ha recibido una ventana de receptor, comprende cuántos bytes se pueden enviar desde que se recibe el último reconocimiento*. En otras palabras, al enviar ventanas de receptor, cada parte intenta regular el flujo de bytes en su dirección e informa a la otra parte del número de bytes (comenzado desde el número del byte para el que se ha enviado el reconocimiento) que está listo a recibir.

La figura 19.11 muestra el flujo de bytes que llega desde el protocolo del nivel superior hacia el búfer de salida de TCP. La entidad TCP recorta la secuencia de segmentos de este flujo de bytes y los prepara para enviarlos hacia otros sockets. En esta figura, la dirección de la transmisión de datos es de derecha a izquierda. En dicho flujo, es posible especificar varias limitantes lógicas. La primera limitante separa los segmentos enviados y para los cuales han llegado reconocimientos. En el otro lado de esta limitante existe la ventana con un tamaño de *W* bytes. Algunos de los bytes que conforman esta ventana son segmentos que han sido enviados pero cuyos reconocimientos todavía no han llegado. La parte restante de la ventana

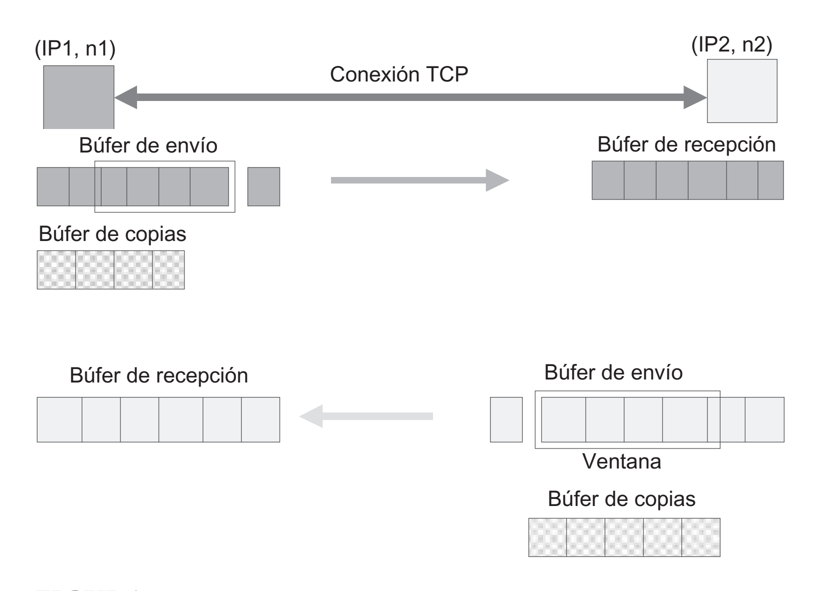


FIGURA 19.10 Sistema de búferes de conexión TCP.

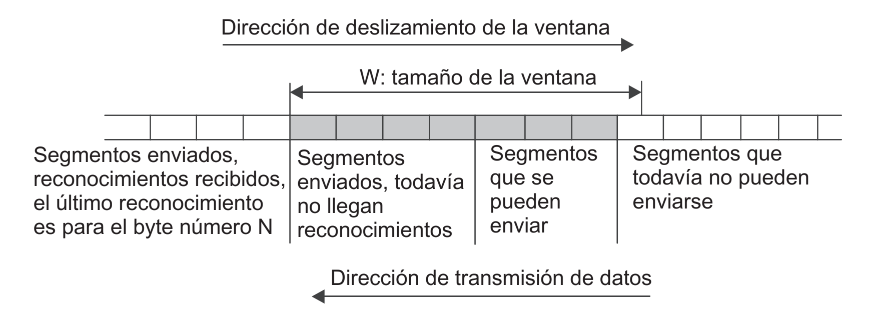


FIGURA 19.11 Implementación del algoritmo de ventana deslizante en TCP.

está conformada por segmentos aún no enviados pero que pueden enviarse debido a que caben dentro de los límites de la ventana. Finalmente, la última limitante especifica el inicio de la secuencia de segmentos que no pueden enviarse hasta que el siguiente reconocimiento llegue y la ventana se mueva hacia la derecha.

Si el tamaño de la ventana es igual a W y el último reconocimiento recibido contenía el valor N, el emisor podrá enviar los segmentos hasta que el byte con el número $N + W$ se ubique en el siguiente segmento. Este segmento va más allá de los límites de la ventana; por lo tanto, es necesario retrasar la transmisión hasta la llegada del siguiente reconocimiento.

19.2.7 Principio de reconocimiento acumulativo

El receptor puede enviar un reconocimiento que confirme la recepción de varios segmentos simultáneamente, a condición de que éstos conformen un flujo continuo de bytes. Por ejemplo (figura 19.12, *a*), supóngase que el búfer se encuentra lleno de manera densa, sin espacio con el flujo de bytes hasta el byte 2 354. Los segmentos (2 355-3 816), (3 817-5 275) y (5 276-8 400), donde los números entre paréntesis designan los números del primero y el último bytes de cada segmento, llegan de manera secuencial a ese búfer. En este caso, es suficiente para el receptor enviar sólo un reconocimiento para los tres segmentos, en el cual se especifique el número 8 401 como un número de reconocimiento. De este modo, el proceso de reconocimiento es acumulativo.

Considérese otro ejemplo (figura 19.12, *b*). Pueden llegar los segmentos al receptor en un orden diferente del cual se enviaron. Esto significa que en el búfer de recepción puede haber una brecha o espacio. Por ejemplo, supóngase que después de los tres segmentos mencionados, llega el segmento (10 567-12 430) en lugar del segmento (8 401-10 566), que se esperaba llegaría a continuación. No es correcto enviar el número 12 431 como el número de reconocimiento, porque esto significaría que todos los bytes hasta el byte 12 430 han sido recibidos. Como se ha presentado una brecha en el flujo de bytes, el receptor puede repetir el reconocimiento 8 401, lo cual indica que todavía espera por la llegada del flujo de bytes a partir del byte 8 401. De este ejemplo se sigue que, en contraste con muchos otros protocolos, TCP reconoce la recepción de una secuencia continua de bytes más que la de bloques de datos por separado.

19.2.8 Tiempo límite de reconocimiento

Sólo para estar seguros, cuando TCP envía un segmento a la red, coloca una copia de este segmento en la cola de reenvío e inicia el cronómetro. Cuando llega un reconocimiento

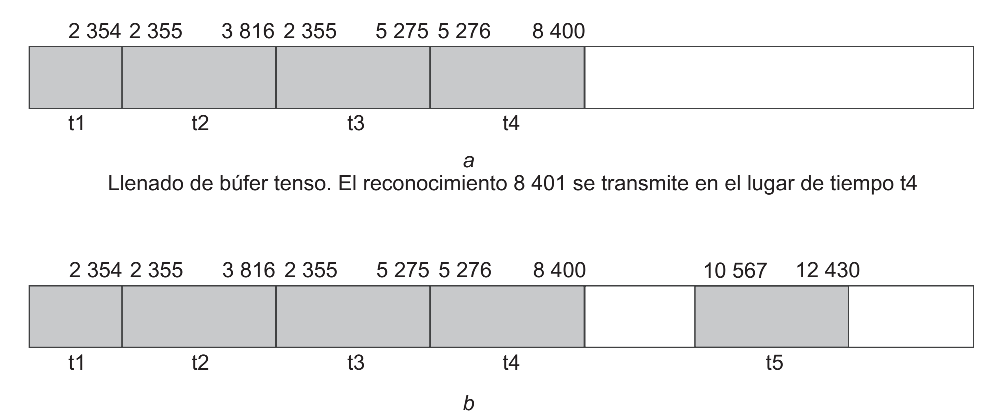


FIGURA 19.12 Principio acumulativo de reconocimiento.

para este segmento, la copia es eliminada de la cola. Si no llega un reconocimiento antes que expire el cronómetro, se reenviará el segmento. Puede ocurrir que el segmento reenviado llegue después de haber sido entregado el segmento inicial. En este caso, se descartará el duplicado.

La selección del tiempo límite o tiempo de espera de reconocimiento es un problema importante, cuya solución influye en el rendimiento de TCP. El tiempo límite no debe ser demasiado breve; debe excluir, siempre que sea posible, los intentos redundantes de retransmisión que reducen el rendimiento efectivo del sistema. Sin embargo, tampoco debe ser demasiado largo, puesto que debe evitar extensos periodos de inactividad relacionados con la espera de reconocimientos perdidos o no existentes.

Cuando se selecciona el valor del tiempo límite, es necesario tomar en cuenta la velocidad y confiabilidad de los enlaces físicos de comunicaciones, sus longitudes y muchos otros factores. En TCP, el valor del tiempo límite se define por medio de un sofisticado algoritmo adaptativo, cuyo concepto principal es el siguiente: durante cada transmisión, se mide el tiempo transcurrido desde el momento de enviar el segmento hasta la llegada de reconocimiento de su recepción. Este tiempo se conoce como **tiempo de viaje redondo** (**RTT**, siglas de **Round Trip Time**). Al promediar los valores medidos del RTT se usan coeficientes de peso que se incrementan con el número secuencial de las medidas. Esto se hace para aumentar la influencia de las últimas mediciones. El valor del tiempo límite es el valor RTT promedio multiplicado por algún coeficiente. La práctica ha demostrado que el valor de este coeficiente debe exceder de 2. En redes en las que el RTT varía de manera significativa, también se toma en cuenta la dispersión del RTT cuando se selecciona el valor del tiempo límite de espera.

19.2.9 Control de la ventana del receptor

El tamaño de la ventana del receptor se relaciona con la disponibilidad del espacio del búfer de datos en la parte receptora. Por lo tanto, las ventanas del receptor por lo general tienen diversos tamaños en diferentes lados de una conexión. Por ejemplo, es lógico esperar que el servidor, que tiene un búfer más grande, enviará una ventana de receptor mayor a la estación de trabajo cliente que la enviada por el cliente hacia el servidor. Según el estado de la red, las partes pueden declarar periódicamente nuevos valores de la ventana de receptor e incrementarlos o disminuirlos de manera dinámica.

Al variar el tamaño de la ventana, es posible que influya en la carga de la red. Cuanto mayor sea la ventana, mayor será la parte de datos sin reconocimiento que pueden enviarse hacia la red; sin embargo, si la cantidad de los datos que llegan es mayor que los que se pueden recibir mediante la entidad TCP, se descartarán aquéllos. Esto producirá intentos en exceso para volver a enviar información y un incremento innecesario en la carga de toda la red en general y sobre el software del TCP en particular.

Por otra parte, especificar una ventana pequeña puede limitar la transmisión de datos a la velocidad determinada por el tiempo requerido por cada segmento que se envía para viajar a través de la red. Para evitar el uso de ventanas pequeñas, algunas implementaciones TCP proponen que el receptor de datos posponga el cambio del tamaño de ventana hasta que el espacio del búfer disponible sea de 20 a 40% de la cantidad máxima de memoria para esta colección. Sin embargo, el emisor tampoco debe apresurarse con el envío de los datos hasta que la ventana del receptor de la parte receptora llegue a ser lo suficientemente grande. Con base en estas consideraciones, los diseñadores del TCP propusieron un método de acuerdo con el cual se declara una ventana grande cuando se establece una conexión, pero su tamaño después se reduce de manera significativa. Existen otros algoritmos de configuración de ventana según los cuales se elige una ventana de tamaño mínimo al establecer una conexión y luego su tamaño se incrementará marcadamente si la red maneja con éxito la carga ofrecida.

El tamaño de la ventana puede ser controlado no sólo por la parte a la que se envía los datos dentro del marco de esta ventana, sino también por la parte emisora. Si esta parte emisora registra una operación no confiable de un enlace de comunicaciones (por ejemplo, los reconocimientos se entregan por lo regular con retardos o se requieren con frecuencia retransmisiones), podrá reducir el tamaño de la ventana por su propia iniciativa. La regla siguiente se aplica en tales casos: se elige el tamaño real de la ventana como el mínimo de dos valores, uno sugerido por el receptor y otro propuesto por el emisor.

La generación de colas en nodos de tránsito (ruteadores) y en nodos terminales (computadoras) indica que la conexión TCP está sobrecargada. En el caso de desbordamiento del búfer en el nodo terminal, cuando TCP envía un reconocimiento, establece un nuevo tamaño reducido de la ventana. Cuando rehúsa la recepción del todo, se especifica una ventana de tamaño cero en el reconocimiento. Sin embargo, incluso después de esto, la aplicación puede enviar un mensaje hacia el puerto que rechaza la recepción de los datos. Para conseguir esto, el mensaje debe ser marcado como urgente. En una situación así, el puerto está obligado a recibir el segmento, incluso si tiene que descargar los datos en el búfer. Después de recibir el reconocimiento con el tamaño cero de la ventana, el protocolo del emisor a veces hace intentos de prueba para continuar el intercambio de datos. Si el protocolo del receptor está listo para recibir información, enviará un reconocimiento con una ventana de tamaño distinto de cero en respuesta a una solicitud así.

Aunque esta descripción del TCP y el UDP se halla lejos de ser detallada, le permite llegar a la conclusión de que uno de ellos (TCP) tiene la complicada e importante tarea de asegurar la confiabilidad de la transmisión de datos a través de una red principalmente no confiable.

Por otro lado, la simplicidad funcional de UDP es la razón para la simplicidad de su algoritmo, su pequeño tamaño y su alta velocidad de operación. En consecuencia, aquellas aplicaciones que ponen en práctica sus mecanismos bastante confiables de mensajería orientada a conexión prefieren utilizar herramientas de transporte menos confiables pero más rápidas para la transmisión de datos a través de la red. El UDP es exactamente una herramienta así en comparación con el TCP. También se podrá utilizar UDP si la alta calidad de los enlaces de comunicaciones asegura un nivel suficiente de confiabilidad sin tener que

establecer conexiones lógicas y reconocimiento de los paquetes que se transmiten. Por último, como TCP está orientado a la conexión, *no puede usarse para difusión o transmisión de datos multidirigida*, en contraste con UDP.

19.3 PROTOCOLOS DE RUTINA

PALABRAS CLAVE: protocolo de enrutamiento, tiempo de convergencia, escalabilidad, sistema autónomo, protocolo de compuerta interior (IGP, Interior Gateway Protocol), protocolo de información de enrutamiento (RIP, Routing Information Protocol), primera trayectoria más corta abierta (OSPF, Open Shortest Path First), de sistema intermedio a sistema intermedio (IS-IS, intermediate system to intermediate system), protocolo de compuerta exterior (EGP, Exterior Gateway Protocol), protocolo de compuerta fronteriza (BGP, Border Gateway Protocol), enrutamiento de inundación, enrutamiento dependiente del evento, enrutamiento de origen, enrutamiento estático, enrutamiento adaptativo, enfoque distribuido, enfoque centralizado, algoritmo del vector de distancia, algoritmo del estado del enlace, anuncio, siguiente hop, BGPv4, técnica de actualizaciones disparadas, técnica de dominación, anuncio de enlaces de ruteador, base de datos del estado del enlace, horizonte dividido y métrica.

19.3.1 Clasificación de protocolos de rutina

Las tablas de ruteo creadas de manera automática aseguran la eficacia de las rutas del paquete a través de la red; debido a ello, los *criterios para seleccionar rutas pueden ser diferentes*. Las redes IP contemporáneas utilizan protocolos de enrutamiento que seleccionan la ruta más corta. En este caso, la distancia pasada por un paquete se interpreta como el número de nodos de tránsito (ruteadores), conocido a menudo como el número de hops. También es posible emplear algún criterio combinado que tome en cuenta los anchos de banda nominales de los ruteadores de conexión de enlaces, confiabilidad del enlace o retardos de enlace.

Un protocolo de enrutamiento debe crear tablas de ruteo coordinadas en los ruteadores, las cuales aseguran la entrega del paquete desde la red de origen hasta la red de destino en un número finito de pasos. También es posible imaginar un par no coordinado de tablas. En esta situación, la tabla de ruteo del ruteador 1 puede especificar que el paquete destinado para la red A debe ser pasado al ruteador 2, mientras que la tabla de ruteo del ruteador 2 puede enviar el mismo paquete al ruteador 1. Los protocolos de enrutamiento contemporáneos aseguran la coordinación de tablas; no obstante, esta propiedad no es absoluta. Por ejemplo, si tienen lugar cambios en la red, como fallas de ruteadores o enlaces de comunicaciones, podrá haber periodos de funcionamiento inestable de la red, causados por una falta temporal de coordinación entre las tablas de ruteo de distintos ruteadores. Como regla, un protocolo de enrutamiento suele requerir algún tiempo, conocido como **tiempo de convergencia**, durante el cual todos los ruteadores de la red, después de varias iteraciones de intercambio de información auxiliar, incluyen los cambios requeridos en sus tablas de ruteo. Como resultado de esta operación, todas las tablas de ruteo se coordinan de nueva cuenta. *Protocolos de enrutamiento diferentes se caracterizan por tener distintos valores de tiempo de convergencia*.

Para que haya una operación con éxito en Internet, las tecnologías de red deben ser **escalables,** lo cual significa que deben asegurar el uso jerárquico de alguna forma. El enrutamiento de Internet sigue dicho principio y divide esta red en **sistemas autónomos**. Como resultado, el enrutamiento en Internet tiene una pronunciada naturaleza jerárquica.

Cualquiera de los protocolos de enrutamiento existentes puede utilizarse en un sistema autónomo. No obstante, entre los sistemas autónomos debe utilizarse el mismo protocolo, como una clase de lenguaje universal, tal como el esperanto, utilizado por los sistemas autónomos para comunicarse entre sí.

En redes IP, el papel de los **protocolos de compuerta interior** (**IGP**) empleados en los sistemas autónomos está delegado a los protocolos siguientes: **protocolo de información de enrutamiento** (**RIP, Routing Information Protocol**), **primera trayectoria más corta abierta** (**OSPF, Open Shortest Path First**) y **de sistema intermedio a sistema intermedio** (**IS-IS, intermediate system to intermediate system**). Otra clase de protocolos, conocidos como **protocolos de compuerta exterior** (**EGP, Exterior Gateway Protocol**), incluyen protocolos de enrutamiento utilizados para seleccionar rutas entre sistemas autónomos. En la actualidad, esta tarea la lleva a cabo el **protocolo de compuerta fronteriza** (**BGP, Border Gateway Protocol**).

Enrutamiento sin tablas

Antes de clasificar los protocolos de enrutamiento, es necesario señalar que también existen métodos en interredes de envío de paquetes, que no requieren la presencia de tablas de ruteo en los ruteadores.

El **enrutamiento de inundación** es el método más simple para pasar paquetes a lo largo de la red. En este caso, cada ruteador pasa el paquete a todos sus vecinos más cercanos, con excepción de aquel desde el cual recibió ese paquete. Naturalmente, este método es el menos eficaz, pues el ancho de banda de la red se desperdicia. Sin embargo, dicho método es factible, porque los puentes y conmutadores hacen con exactitud este tipo de envío en relación con las tramas cuyas direcciones son desconocidas.

Otra variante de enrutamiento sin tablas de ruteo es el **enrutamiento dependiente del evento**, de acuerdo con el cual el paquete es enviado a una red de destino específica junto con la ruta que haya producido una entrega con éxito (para la dirección de destino dada). Este método de enrutamiento se utilizó cuando Internet empezaba a crecer. De acuerdo con dicho método, antes de enviarse un paquete, un eco o reenvío de ICMP solicita ser enviado a todos los vecinos o a varios; luego, con base en el tiempo de las respuestas que llegaban al eco, se elegía al vecino que tuviera el tiempo de respuesta mínimo.

Tal método es adecuado para usarlo en redes que funcionan según los protocolos orientados a conexión. La solicitud para establecer una conexión puede enviarse de manera simultánea a varios vecinos y el reconocimiento debe enviarse al primer vecino que envía una respuesta.

Otro tipo de enrutamiento que no requiere tablas de ruteo es el **enrutamiento fuente** o **de origen**. En este caso, el emisor coloca información en el paquete acerca de los ruteadores de tránsito que deben participar en la entrega del paquete a la red de destino. Con base en esta información, cada ruteador lee la dirección del siguiente ruteador y, si es la dirección de su vecino más cercano, pasa el paquete a él para procesamiento adicional. El asunto de determinar la ruta exacta a lo largo de la cual el paquete viaja a través de la red permanece abierto. Esta trayectoria la puede especificar un administrador de forma manual o determinarla de forma automática el nodo emisor, el cual, en este caso, debe soportar algún protocolo de enrutamiento. En esta situación, dicho protocolo debe informar al emisor acerca del estado y topología de la red. El enrutamiento de origen fue probado en experimentos iniciales de Internet y ha sido preservado como una opción de IPv4 prácticamente sin utilizar. En IPv6,

el enrutamiento de origen es uno de los modos estándar de envío de paquetes y existe un encabezado especial para poner en práctica este modo.

Enrutamiento adaptativo

Cuando el enrutamiento se lleva a cabo con base en tablas, existe enrutamiento *estático* y *adaptativo* (o dinámico).

En caso de enrutamiento estático, se crean e introducen tablas de ruteo en cada ruteador *de forma manual por el administrador de la red*. Todos los registros en la tabla de ruteo tienen el estado de estático, lo cual significa que permanecen en vigor de manera infinita. Cuando el estado de algún elemento de la red cambia, el administrador debe introducir manualmente el cambio apropiado en las tablas de ruteo de aquellos ruteadores influidos por él. Por ejemplo, puede ser necesario modificar una ruta o rutas para los paquetes, lo cual debe hacerse en cuanto sea posible; de otra forma, la red puede funcionar de manera incorrecta.

El **enrutamiento adaptativo** asegura la *actualización automática de las tablas de ruteo* cuando se modifica la configuración de la red. La actualización de las tablas de enrutamiento es precisamente la tarea para la que son necesarios los protocolos de enrutamiento. Estos protocolos funcionan de acuerdo con algoritmos que permiten a todos los ruteadores coleccionar información referente a la topología del enlace en la red y reflejar de manera flexible todos los cambios en la configuración de enlace en el momento. Si se utiliza el enrutamiento activo, las tablas de ruteo por lo general contendrán información sobre el intervalo durante el cual cada ruta individual permanece válida. Este intervalo se conoce como el *tiempo de vida* de la ruta (TTL). Si el periodo TTL ha expirado y no se ha confirmado la existencia de la ruta por el protocolo de enrutamiento, una ruta así se considera inviable y los paquetes no se enviarán a lo largo de ella.

Los protocolos de enrutamiento se clasifican en protocolos distribuidos y centralizados.

- Cuando se utiliza un **enfoque distribuido**, la red no contiene ningún ruteador dedicado que recolectaría y resumiría información acerca de la topología de la red. Por el contrario, este trabajo se distribuye entre todos los ruteadores de la red. Cada ruteador construye su tabla de ruteo con base en los datos recibidos de acuerdo con el protocolo de enrutamiento de otros ruteadores de la red.
- Cuando se emplea un **enfoque centralizado**, existe un ruteador dedicado en la red, el cual recolecta toda la información relacionada con la topología de la red y su estado suministrada por otros ruteadores. Luego este ruteador dedicado, en ocasiones conocido como *servidor de ruteo*, puede seleccionar una de las posibles variantes de comportamiento. Puede construir tablas de enrutamiento para todos los ruteadores restantes de la red y luego distribuirlas en la red de manera que todos los ruteadores recibirán su propia copia o tabla de ruteo; después, puede tomar decisiones acerca del envío de paquetes por sí mismo.

> Los protocolos de enrutamiento actualmente utilizados en redes se clasifican como protocolos adaptativos distribuidos.

Los algoritmos de enrutamiento adaptativo deben satisfacer varios requerimientos importantes. En primer lugar, las rutas seleccionadas por estos algoritmos deben ser eficaces si no es que óptimas. En segundo lugar, los algoritmos deben ser lo bastante simples para que

su implementación no desperdicie los recursos de la red. En particular, no deben requerir una enorme cantidad de cálculos o generar un tráfico de control intenso. Por último, los algoritmos de enrutamiento han de caracterizarse por la propiedad de convergencia; es decir, siempre deben coordinar la construcción de las tablas de ruteo para asegurar la convergencia de todos los ruteadores de la red en un tiempo razonable.

Los algoritmos de enrutamiento adaptativo utilizados en las redes de computadoras en la actualidad están divididos en dos grupos, cada uno de los cuales implementa uno de los tipos de algoritmos siguientes:

- Algoritmos de vector de distancia.
- Algoritmos de estado del enlace.

Algoritmos de vector de distancia

En los **algoritmos de vector de distancia** (**DVA**, siglas de **Distance Vector Algorithms**), cada ruteador transmite periódicamente el vector, cuyos componentes son las distancias desde este ruteador a todas las redes que conoce. Los paquetes enviados mediante protocolos de enrutamiento por lo regular se llaman **anuncios**, porque el ruteador los utiliza para informar a los otros ruteadores en la estructura de la red que conoce. Como regla, la distancia en un DVA se interpreta como el número de hops; sin embargo, también es posible otra métrica, que toma en cuenta no sólo el número de nodos de tránsito (ruteadores), sino también el ancho de banda del enlace que conecta dos ruteadores adyacentes.

Una vez recibido un vector desde su vecino, el ruteador incrementa las distancias especificadas en este vector por un valor igual a la distancia de dicho vecino y complementa el vector con información inherente a otras redes conocidas para él. La información acerca de estas redes puede obtenerse directamente cuando se conectan a puertos del ruteador actual, o de anuncios similares recibidos desde otros ruteadores. Después de eso, el ruteador transmite este nuevo valor del vector hacia la red. Al final, cada ruteador obtendrá de sus vecinos información acerca de todas las redes conectadas a Internet y las distancias a ellas. Luego de esto, de varias rutas alternativas para cada red, elegirá la que tiene el valor métrico más pequeño. El ruteador que ha pasado información relacionada con esta ruta es marcado en la tabla de ruteo como el **hop siguiente**.

Los DVA funcionan de manera eficaz sólo en redes pequeñas. En redes grandes, sobrecargan los enlaces de comunicaciones con un tráfico periódico intenso. Además, los cambios de configuración pueden no ser procesados de manera correcta de acuerdo con este algoritmo, pues los ruteadores no tienen la información exacta acerca de la topología de los enlaces de red. Por el contrario, sólo tienen información generalizada, el vector de distancia; además, éste contiene información mediada, que no se recibió directamente.

Entre los protocolos basados en DVA, RIP es el más ampliamente utilizado. Este protocolo tiene dos versiones: RIP IP, destinado para IP, y el RIP IPX, que trabaja con IPX.

Algoritmos de estado del enlace

Los **algoritmos de estado del enlace (LSA**, siglas de **Link State Algorithms)** proporcionan a cada ruteador información suficiente para construir una gráfica exacta de los enlaces de la red. Todos los ruteadores funcionan con base en la misma gráfica, lo que hace el proceso de enrutamiento más estable en contra de los cambios de configuración.

Cada ruteador utiliza la gráfica de red para hallar rutas hacia cada una de las redes incluidas en la interred. Estas rutas son las óptimas de acuerdo con algún criterio específico.

Para encontrar el estado de los enlaces de comunicaciones conectados a sus puertos, el ruteador intercambia de manera periódica breves paquetes *HELLO* con sus vecinos más cercanos.

Los anuncios concernientes al estado del enlace no se repiten periódicamente, como en el caso de los protocolos DVA. Por el contrario, se transmiten sólo si se detectó un cambio de estado de un enlace específico al intercambiar los mensajes *HELLO*. Como resultado, el tráfico de control generado por los protocolos LSA es bastante menos intenso que el producido por los protocolos DVA.

Ejemplos de protocolos LSA son el protocolo IS-IS de la pila OSI (este protocolo también se utiliza en la pila TCP/IP), el protocolo OSPF de la pila TCP/IP y el protocolo de servicios de enlace NetWare de la pila Novell.

Uso de varios protocolos de enrutamiento

Varios protocolos de enrutamiento pueden funcionar de manera simultánea en la misma red (figura 19.13). Esto significa que en algunos ruteadores de red (pero no necesariamente en todos) se encuentran instalados y en ejecución varios protocolos de enrutamiento. Desde luego, únicamente los protocolos nombrados de manera similar utilizan la red al interactuar. Esto significa que si el ruteador 1 soporta los protocolos RIP y OSPF, el ruteador 2 soportará sólo RIP y el ruteador 3 únicamente sostendrá OSPF, el ruteador 1 interactuará con el ru-

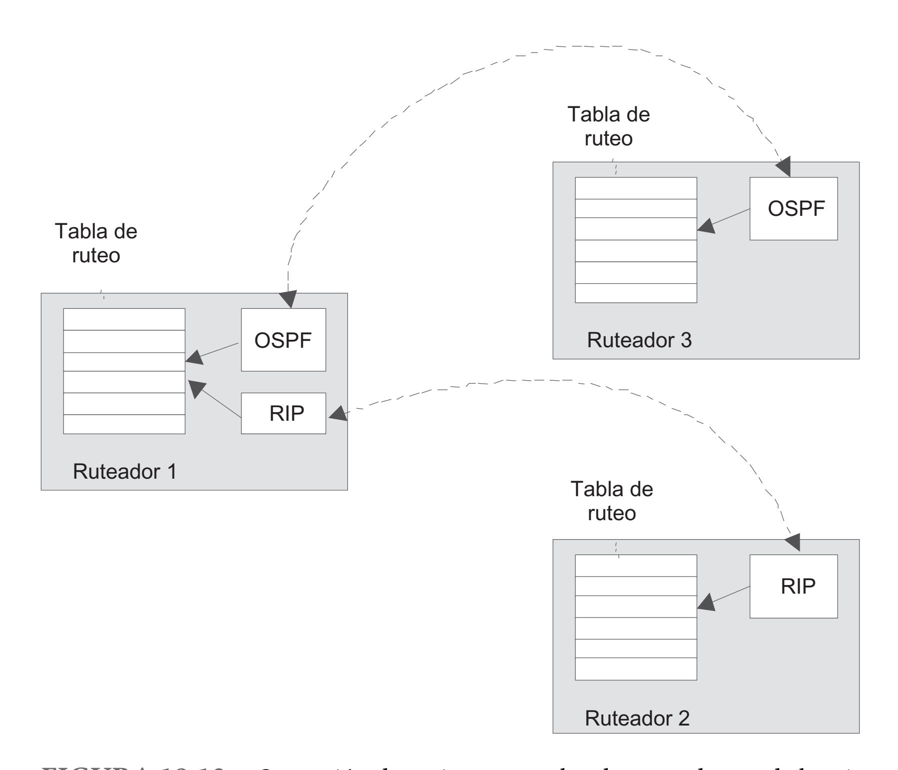


FIGURA 19.13 Operación de varios protocolos de ruteo dentro de la misma red.

teador 2 según RIP y con el ruteador 3 según OSPF; a su vez, los ruteadores 2 y 3 no podrán comunicarse de forma directa.

En un ruteador que soporta varios protocolos, cada registro en la tabla de ruteo es resultado de la operación de uno de estos protocolos. Si la información en una red específica es suministrada por varios protocolos, para asegurar la no ambigüedad de la selección de ruta se establecen prioridades de protocolo; de otro modo, los datos desde diferentes protocolos pueden producir distintas rutas eficaces. Como regla, se da preferencia a los protocolos LSA porque, en comparación con los protocolos DVA, tienen información detallada acerca de la red DVA. En algunos sistemas operativos, las formas para exhibir o imprimir una tabla de ruteo contienen marcas especiales que especifican el protocolo de enrutamiento utilizado para obtener cada registro. Incluso cuando no se exhibe esta marca, siempre se encuentra en la representación interna de la tabla de ruteo. De manera predeterminada, cada protocolo de enrutamiento que se ejecuta en un ruteador específico distribuye solamente la información recibida por el ruteador de acuerdo con dicho protocolo. De esta forma, si el ruteador obtiene información respecto a alguna red desde RIP, utilizará el mismo protocolo para distribuir anuncios de esta ruta sobre la red.

No obstante, cabe formular la siguiente pregunta: "¿cómo intercambian los ruteadores que soportan distintos protocolos de enrutamiento utilizados en la interred la información de enrutamiento para hacer que todas las redes constituyentes de la interred se encuentren disponibles?" Para permitir que el ruteador use un protocolo de enrutamiento con el fin de distribuir información de enrutamiento recibida mediante el empleo de otro protocolo de enrutamiento, es necesario establecer el modo interno específico de su operación, llamado a menudo *modo redistribuido*. Este modo asegura que en un protocolo específico se pueden utilizar no sólo sus registros "nativos" desde las tablas de ruteo, sino también otros registros obtenidos al emplear otros protocolos de enrutamiento especificados en el curso de la configuración.

Como puede verse de la descripción, el uso de varios protocolos de enrutamiento dentro de los límites de la misma interred no es una tarea trivial. Un administrador debe llevar a cabo tareas específicas relacionadas para configurar cada ruteador. Como es natural, para grandes redes heterogéneas es necesaria una solución principalmente distinta.

Una solución así se encontró para Internet, la interred heterogénea más grande hasta ahora.

Protocolos de compuerta exterior e interior

Aparte de la estructura organizacional de Internet descrita en el *capítulo 5* y la determinación de la división de esta red en redes de varios ISP, Internet está conformada por sistemas autónomos.

Un *sistema autónomo* es un conjunto de redes vinculadas mediante una dirección administrativa común, que garantizan una política de enrutamiento común para todos los ruteadores incluidos dentro del sistema autónomo. Como regla, un sistema autónomo está controlado por un solo ISP. Este ISP determina cuáles protocolos de enrutamiento se utilizan en un sistema autónomo específico y cómo se distribuye y redistribuye la información de enrutamiento entre ellos. Los ISP de alto nivel y compañías grandes pueden representar sus interredes como conjuntos de varios sistemas autónomos. El registro del sistema autónomo está centralizado de una forma similar al registro de las direcciones IP y los nombres DNS.

Todos los sistemas autónomos están numerados de manera central. El número de sistema autónomo comprende 16 bits, pero no está relacionado con los prefijos IP de las redes que conforman el sistema autónomo.

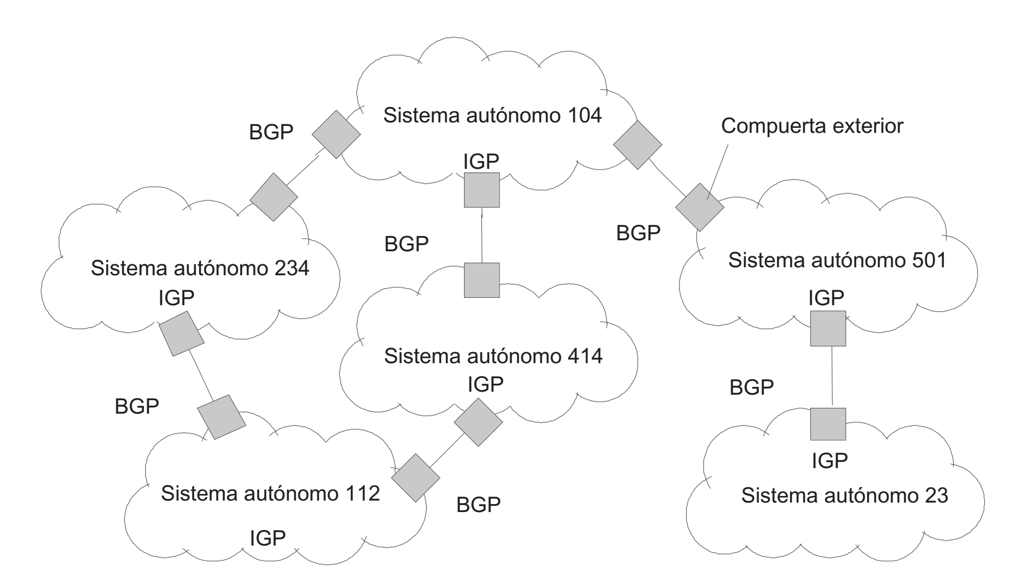


FIGURA 19.14 Sistemas autónomos de Internet.

De acuerdo con este concepto, Internet tiene el aspecto de un conjunto de sistemas autónomos interconectados, cada uno de los cuales abarca redes interrelacionadas (figura 19.14).

El objetivo principal de dividir Internet en sistemas autónomos consiste en asegurar un enfoque de multinivel al enrutamiento. Antes de la introducción de los sistemas autónomos, el enrutamiento suponía un enfoque de dos niveles —en la capa de la red, la ruta estaba extendida entre grupos de nodos (redes) y el enrutamiento interredes estaba asegurado mediante tecnologías de capa inferior. Esto significa que la ruta define la secuencia del paso en las redes.

Con la llegada de los sistemas autónomos apareció el tercer nivel de enrutamiento: la ruta se elige primero en el nivel de los sistemas autónomos y luego en el de sus redes constituyentes.

Los sistemas autónomos están conectados mediante **compuertas exteriores**.[4] Lo importante es que entre compuertas exteriores solamente se permite un protocolo de enrutamiento; además, no debe ser un protocolo arbitrario. Por el contrario, debe ser el protocolo adoptado por la comunidad de Internet como el protocolo estándar para compuertas exteriores. Tales protocolos de enrutamiento se denominan **protocolos de compuerta exterior** (**EGP, Exterior Gateway Protocols**). Por el momento, sólo existe un protocolo de enrutamiento así: BGPv4. Todos los protocolos (por ejemplo, RIP, OSPF y IS-IS) pertenecen a la clase de **protocolos de compuerta interior** (**IGP, Interior Gateway Protocols**).

El EGP es responsable de la selección de la ruta como una secuencia de sistemas autónomos. Como resultado del ruteador siguiente, se especifica la dirección del punto de acceso en el siguiente sistema autónomo.

A los IGP se atribuye la ruta *dentro de un sistema autónomo*. En sistemas autónomos de tránsito se especifica la secuencia exacta de ruteadores desde el punto de acceso hasta el punto donde la ruta abandona este sistema autónomo.

---

[4] De ahora en adelante, los términos *ruteador* y *compuerta* se utilizarán como sinónimos, para pagar tributo a la terminología tradicional de Internet sin olvidar la terminología más reciente.

Los sistemas autónomos forman la columna vertebral de Internet. El concepto de sistemas autónomos oculta de los administradores troncales de Internet los programas de enrutamiento de paquetes hasta el nivel de red inferior. Para el administrador troncal, los protocolos de enrutamiento utilizados dentro de los sistemas autónomos no son de importancia. El único protocolo de enrutamiento que importa es **BGPv4**.

19.3.2 Protocolo de información de enrutamiento

Construcción de una tabla de enrutamiento

El **protocolo de información de enrutamiento (RIP, Routing Information Protocol)** es un IGP basado en el algoritmo DVA y es uno de los protocolos de enrutamiento más antiguos, el cual, gracias a la simplicidad de su implementación, se utiliza ampliamente en redes de computadoras.

Para redes IP existen dos versiones de RIP: RIPv1 y RIPv2. La primera versión, RIPv1, no soporta máscaras; en, RIPv2 distribuye información acerca de máscaras de redes; por lo tanto, es mucho más adecuado para los requerimientos de hoy en día. No obstante, como el proceso de construir una tabla de ruteo usada por RIPv2 no es fundamentalmente distinto del utilizado por RIPv1, por simplicidad, se escribirá este proceso en el ejemplo de la primera versión.

Las versiones RIP permiten utilizar diferentes tipos de métricas para definir la distancia hacia la red. Por ejemplo, es posible emplear la métrica más simple, hops, o tipos de métricas más complejos que tomen en cuenta los anchos de banda de la red, los retardos introducidos y la confiabilidad de la red (es decir, correspondientes a las banderas *D, T* y *R* en el campo *ToS* del paquete IP), además de cualquier combinación de estas métricas. La métrica debe caracterizarse por la propiedad aditiva, a saber: la métrica de la ruta combinada debe ser igual a la suma de las métricas que caracterizan los componentes de esta ruta. En la mayoría de las implementaciones de RIP, se utiliza la métrica más simple, o sea, el número de hops (es decir, ruteadores de tránsito a través de los cuales el paquete tiene que pasar para alcanzar la red de destino).

Considérese el proceso de construcción de una tabla de ruteo utilizando RIP en el ejemplo de la interred mostrada en la figura 19.15.

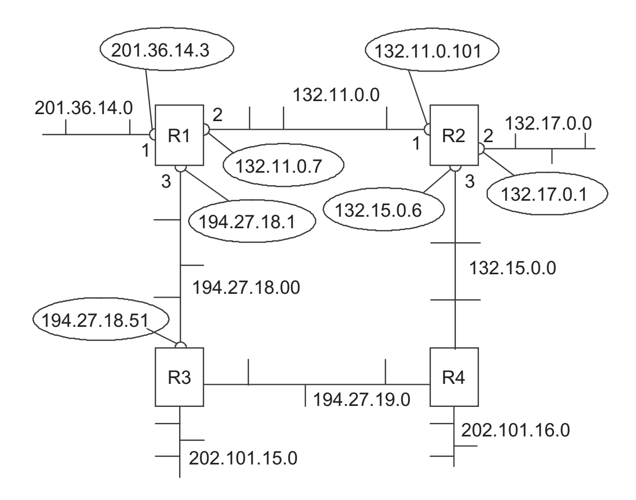


FIGURA 19.15 Red construida sobre compuertas RIP.

Etapa 1. Creación de tablas mínimas

La red considerada consta de ocho redes IP conectadas por cuatro ruteadores con los identificadores siguientes: R1, R2, R3 y R4. Los ruteadores que funcionan de acuerdo con RIP deben tener identificadores; sin embargo, éstos no se requieren para la operación del protocolo, porque no se pasan en los mensajes RIP.

En el estado inicial, el software de la pila TCP/IP crea de manera automática la **tabla de ruteo mínima**, que toma en cuenta sólo redes conectadas directamente. En la figura 19.15, las direcciones de los puertos del ruteador están colocadas en óvalos para que contrasten de las direcciones de red.

La tabla 19.1 permite evaluar el aspecto de la tabla de ruteo mínima del ruteador R1.

La tabla de ruteo mínima para otros ruteadores tendrá un aspecto parecido. Por ejemplo, la tabla de ruteo del ruteador R2 contendrá tres registros (tabla 19.2).

Etapa 2. Envío de tablas mínimas a los vecinos

Después de la inicialización, cada ruteador comienza a enviar a sus vecinos mensajes RIP que contienen su tabla mínima.

Los mensajes RIP se pasan en paquetes UDP e incluyen dos parámetros para cada red: su dirección IP y la distancia a esta red desde el ruteador que transmite este mensaje.

Los vecinos son los ruteadores a los cuales el ruteador actual puede pasar el paquete IP de manera directa sin utilizar ruteadores de tránsito. Por ejemplo, para el ruteador R1, los vecinos son R2 y R3, mientras que para R4 serán R2 y R3.

Así, el ruteador R1 pasa el siguiente mensaje a R2 y R3:

Red 201.36.14.0, distancia 1.
Red 132.11.0.0, distancia 1.
Red 194.27.18.0, distancia 1.

TABLA 19.1 Tabla de ruteo mínima del ruteador R1

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

TABLA 19.2 Tabla de ruteo mínima del ruteador R2

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
132.11.0.0	132.11.0.101	1	1
132.17.0.0	132.17.0.1	2	1
132.15.0.0	132.15.0.6	3	1

TABLA 19.3 Agregación de registros para la tabla de ruteo del ruteador R1

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.17.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	2	2
~~132.11.0.0~~	~~132.11.0.101~~	~~2~~	~~2~~
~~194.27.18.0~~	~~194.27.18.51~~	~~3~~	~~2~~

Etapa 3. Recepción de mensajes RIP desde los vecinos y procesamiento de la información de enrutamiento

Después de recibir mensajes similares desde los ruteadores R2 y R3, el ruteador R1 incrementa cada valor de métrica recibido en uno y “memoriza” la información a través de qué puerto y desde qué ruteador fue recibida la nueva información. La dirección de este ruteador se convertirá en la dirección del siguiente ruteador si este registro se incluirá en la tabla de ruteo. A continuación, el ruteador comienza a comparar la nueva información con la almacenada en su tabla de ruteo (tabla 19.3).

Los registros con los números del 4 al 9 se recibieron desde los ruteadores vecinos y son candidatos para insertarlos en la tabla. Sin embargo, sólo los registros 4-7 se agregarán en la tabla de ruteo, pero los registros 8 y 9 no. Esto ocurre debido a que tales registros contienen datos acerca de redes que se encuentran en la tabla de ruteo del ruteador R1, y la distancia especificada en estos registros es mayor que la distancia determinada en los registros existentes de la tabla de ruteo.

RIP reemplaza el registro para una red específica sólo cuando la nueva información tiene una mejor métrica (es decir, la distancia en los hops es más pequeña) que la existente. Como resultado, sólo un registro en cada red permanece en la tabla de ruteo. Incluso si hay varias trayectorias hacia la misma red caracterizadas por iguales distancias, únicamente un registro permanecerá en la tabla de ruteo: el primero en llegar a este ruteador. Existe una excepción a dicha regla: si ha llegado una información peor acerca de una red específica desde el mismo ruteador, con base en cuyo mensaje fue creado el registro actual, el registro con la peor métrica reemplazará al registro con la mejor. Esto ocurre porque la situación en la red ha cambiado a la peor opción, y el ruteador que puede comprobarse informa acerca de ello.

Otros ruteadores de red llevan a cabo operaciones semejantes para la nueva información que reciben.

TABLA 19.4 Actualización de la tabla de ruteo del ruteador R1

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
~~132.15.0.0~~	~~194.27.18.51~~	~~3~~	~~3~~
194.27.19.0	194.27.18.51	3	2
~~194.27.19.0~~	~~132.11.0.101~~	~~2~~	~~3~~
~~202.101.15.0~~	~~194.27.18.51~~	~~3~~	~~2~~
202.101.16.0	132.11.0.101	2	3
~~202.101.16.0~~	~~194.27.18.51~~	~~3~~	~~3~~

Etapa 4. Envío de una nueva tabla a los vecinos

Cada ruteador envía su nuevo mensaje RIP a sus vecinos, en el cual coloca los datos acerca de todas las redes conocidas para él, tanto las conectadas directamente como las más remotas, para las que el ruteador ha recibido información en mensajes RIP de otros ruteadores.

Etapa 5. Recepción de nuevos mensajes RIP desde los vecinos y procesamiento de la información recibida

La etapa 5 repite la etapa 3: todos los ruteadores reciben mensajes RIP y procesan la información contenida ahí. Luego, de acuerdo con esta información, corrigen sus tablas de ruteo.

Considérese cómo el ruteador R1 lleva a cabo esta operación (tabla 19.4).

En esta etapa, el ruteador R1 ha recibido información desde el ruteador R3 referente a la red 132.15.0.0, que recibió ese ruteador en la etapa anterior desde el ruteador R4. El ruteador R1 ya tiene conocimiento acerca de la red 132.15.0.0 y la información anterior tiene la mejor métrica; por consiguiente, la nueva información acerca de esta red es descartada.

La información acerca de la red 202.101.16.0 la recibió el ruteador R1 por primera vez y llegó simultáneamente desde dos vecinos, R3 y R4. Como las métricas en ambos mensajes son iguales, el registro que llegó primero se incluirá en la tabla de ruteo. En este ejemplo, el ruteador R2 tomó la delantera sobre el ruteador R3 y fue el primero en enviar su mensaje RIP al ruteador R1.

Si los ruteadores repiten periódicamente las etapas de envío y procesamiento de mensajes RIP, entonces en un periodo finito, el modo de enrutamiento correcto se establecerá dentro de la red. Aquí, de acuerdo con el modo de enrutamiento correcto, se crearán tablas de ruteo en las que todas las redes sean alcanzables desde cualquier red utilizando alguna ruta eficaz. Los paquetes alcanzarán sus destinos y no se perderán en rutas cíclicas semejantes a la formada por los ruteadores R1-R2-R3-R4 (figura 19.15).

Si todos los ruteadores de la red, todas sus interfases y todos los enlaces de comunicaciones que los conectan están en operación, raras veces enviarán anuncios de acuerdo con RIP, por ejemplo, uno por día. Sin embargo, los cambios en la estructura de la red se presentan constantemente. El uso de ruteadores y enlaces de comunicación puede cambiar y también pueden agregarse o eliminarse de la red existente nuevos ruteadores y enlaces de comunicación.

Para adaptarse a esos cambios en la estructura de la red, RIP utiliza varios mecanismos.

Adaptación de los ruteadores RIP a los cambios de estado de la red

Los ruteadores RIP se adaptan con facilidad a las nuevas rutas: simplemente se pasa la nueva información en el siguiente mensaje enviado a sus vecinos. De este modo, la nueva información llega a conocerse de manera gradual para todos los ruteadores de la red; no obstante, la adaptación a las consecuencias negativas relacionadas con la pérdida de alguna ruta es más difícil. Esto se debe a que los mensajes RIP no contienen un campo que especificaría que la ruta a esta red ya no existe.

Para informar a los ruteadores que alguna ruta ya no es válida se emplean los dos mecanismos siguientes de notificación:

- Expiración de la ruta TTL.
- Notificación de que una distancia especial (infinita) hacia la red ha dejado de estar disponible.

Para instalar el mecanismo de **Expiración de la ruta TTL**, cada registro de la tabla de ruteo (además de los registros de la tabla de envío puente/conmutador) recibida de acuerdo con RIP tiene un TTL limitado. Cuando llega otro mensaje RIP, que confirma la validez de un registro específico, el cronómetro TTL se restablece a su estado inicial y entonces disminuye en uno cada segundo. Si un nuevo mensaje en esta ruta no llega dentro del tiempo límite, esta ruta se marca como válida.

El tiempo límite está relacionado con el periodo de los vectores de difusión en la red. En RIP, este periodo es de 30 segundos y el valor de tiempo límite es seis veces la extensión de dicho periodo (es decir, 180 segundos). La reserva séxtuple de tiempo es necesaria para asegurar que una red específica ha dejado de estar disponible y que la falta de conectividad no la causa la pérdida de mensajes RIP. Obsérvese que es posible la pérdida de los mensajes RIP, pues RIP utiliza el protocolo de transporte UDP, el cual no asegura la transmisión confiable de los mensajes.

Si cualquier ruteador falla y deja de enviar mensajes acerca de las redes que pueden alcanzarse a través de él, después de 180 segundos todos los registros generados por ese ruteador serán invalidados en sus vecinos más cercanos. Después de eso, este proceso se repetirá para los vecinos de los vecinos más cercanos. Esta vez, los registros inválidos se descartarán después de 360 segundos, pues durante los primeros 180 segundos los vecinos más cercanos del ruteador fallido todavía transmiten información acerca de ese ruteador.

La información relacionada con la red que deja de estar disponible debido a la falla del ruteador se propaga lentamente a través de la red. Debido a esto, se elige el periodo de transmisión o difusión tan pequeño como de 30 segundos.

El **mecanismo de tiempo límite** funciona cuando el ruteador no puede informar a sus vecinos respecto a la ruta fallida, ya sea porque también ha fallado o debido a la falla del enlace de comunicaciones a través del cual sería posible transmitir el mensaje.

Cuando es posible enviar un mensaje, los ruteadores RIP no utilizan ningún atributo especial en el mensaje; en vez de ello, especifican una distancia infinita hacia la red. Nótese que en RIP, esta distancia es de 16 hops. Si se usa otra métrica en lugar de los hops, es necesario especificar un valor de esta métrica que se consideraría infinito por el ruteador. Considérese lo que ocurre cuando un ruteador recibe un mensaje en el que alguna red está caracterizada por una distancia infinita (16 hops). Obsérvese que si esa red está a 15 hops de distancia, el resultado será el mismo, pues el ruteador incrementa el valor recibido por 1. Una vez que ha recibido un mensaje a sí, el ruteador debe verificar si esta información "negativa" llegó desde el ruteador que envió una vez el mensaje con base en el cual el registro en la red en cuestión se incluyó en la tabla de ruteo. Si éste es el caso, la información se considerará confiable y la ruta se marcará como no disponible.

Se elige un pequeño valor de esta naturaleza para la distancia "infinita" debido a que en algunos casos las fallas de enlace causan periodos prolongados de operación incorrecta de los ruteadores RIP. El comportamiento incorrecto se manifiesta como la circulación infinita de paquetes en ciclos cerrados de la red. Cuanto más pequeño sea el valor utilizado como "infinito", más breves serán tales periodos de operación incorrecta de la red.

EJEMPLO *Considérese un caso de ciclo cerrado infinito de paquete en la red de ejemplo en la figura 19.15.*

Supóngase que el ruteador R1 ha detectado que ha perdido su conectividad a la red conectada directamente 201.36.14.0. Por ejemplo, esto puede ocurrir debido a la falla de la interfase 201.36.14.3. El ruteador R1 ha marcado a la red 201.36.14.0 como no disponible en su tabla de ruteo. En el peor de los casos, el ruteador detecta este hecho de inmediato después de enviar mensajes RIP programados regularmente. En este caso, toma casi 30 segundos antes de comenzar el nuevo ciclo de sus anuncios en los cuales tiene que informar a sus vecinos que la distancia a la red 201.36.14.0 llega tener un valor 16.

Cada ruteador funciona con base en su reloj interno, sin sincronizar su operación de envío de anuncios a otros ruteadores. Por lo tanto, es muy probable que el ruteador R2 tomara la delantera sobre R1 y pasara su mensaje antes que R1 tuviera tiempo para pasar la información de la no disponibilidad de la red 201.36.14.0. El mensaje enviado por el ruteador R2 puede contener datos generados por el registro desde su tabla de ruteo (tabla 19.5).

Este registro fue recibido desde el ruteador R1 y era correcto hasta la falla de la interfase 201.36.14.3. Dicho registro se convirtió en uno no válido; sin embargo, el ruteador R2 no ha sido informado acerca de esto todavía.

Ahora el ruteador R1 recibirá nueva información respecto a la red 201.36.14.0. De acuerdo con tal información, esta red puede alcanzarse a través del ruteador R2 con una métrica de 2. Anteriormente, R1 también recibió la misma información desde el ruteador R2; no obstante, el ruteador ignoraba dicha información debido a

TABLA 19.5 Registro en la tabla de ruteo del ruteador R2

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
201.36.14.0	132.11.0.7	1	2

TABLA 19.6 Registro en la tabla de ruteo del ruteador R1

Número de red	Dirección del siguiente ruteador	Puerto	Distancia
201.36.14.0	132.11.0.101	2	3

que su propia métrica para 201.36.14.0 era mejor. Ahora, R1 debe recibir los datos inherentes a la red 201.36.14.0 desde R2 y reemplazar el registro en la tabla de ruteo, y marcar esta red como no disponible (tabla 19.6).

Como resultado, se generó un "loop" o ciclo cerrado de enrutamiento en la red: los paquetes enviados a los nodos de la red 201.36.14.0 pasarán por el ruteador R2 hacia el ruteador R1, y el ruteador R1 los regresará hacia el ruteador R2. Los paquetes IP circularán en este ciclo hasta que expire el TTL para cada paquete.

El ciclo de enrutamiento existirá en la red durante un tiempo relativamente largo. Considérense los periodos que son múltiplos del TTL de los registros de la tabla de ruteo:

- De 0 a 180 segundos. *Después de la falla de la interfase, los registros incorrectos se preservarán en tablas de ruteo de los ruteadores R1 y R2. El ruteador R2 continuará proporcionando al ruteador R1 su registro acerca de la red 201.36.14.0 con métrica 2, debido a que el TTL de este registro todavía no ha expirado. En consecuencia, los paquetes se ubicarán en el loop.*
- De 180 a 360 segundos. *Al inicio de este periodo, el TTL del registro acerca de la red 201.36.14.0 con métrica 2 expirará en el ruteador R2 porque R1, durante el periodo anterior, le envió sus anuncios relacionados con la red 201.36.14.0 con una peor métrica, y no podían confirmar este registro. Ahora, R2 recibe un registro acerca de la 201.36.14.0 desde el ruteador R1 caracterizado por la métrica 3. Ello transforma esto en el registro con métrica 4. Por otra parte, R1 no recibe nuevos mensajes desde R2 respecto a la red 201.36.14.0 con métrica 2; por lo tanto, el TTL de su registro comienza a ser disminuido. Y los paquetes continúan circulando en el loop o ciclo cerrado.*
- De 360 a 540 segundos. *El TTL del registro concerniente a la red 201.36.14.0 con métrica 3 en el ruteador R1 expira. Los ruteadores R1 y R2 intercambian una vez más sus papeles: ahora R2 suministra a R1 información obsoleta acerca de la trayectoria hacia la red 201.36.14.0; sin embargo, esta vez la métrica será 4 y el ruteador R1 se incrementaría por 1 y se convertiría en 5. Asimismo, continuará la circulación de los paquetes en el ciclo cerrado.*

Si no fuera por la selección de la distancia "infinita" de 16, este proceso continuaría indefinidamente. Para ser más precisos, seguiría hasta que la longitud del campo de distancia fuera excedida, lo que sería sobrepasado después del siguiente intento para incrementar la distancia.

Por último, el ruteador R2 en la siguiente etapa del proceso descrito regresará la métrica 15 desde el ruteador R1, el cual, después de incrementarla, la deja en 16. El ruteador R2 registrará entonces que la red es inalcanzable. El periodo de operación inestable de la red tardó ¡36 minutos!

La limitación de 15 hops reduce el área de aplicabilidad de RIP a las redes en las que el número de ruteadores de tránsito no excede 15. Para redes más grandes, es necesario utilizar otros protocolos de enrutamiento, como OSPF, o dividir la red en áreas autónomas.

El ejemplo descrito ilustra la principal razón de la operación inestable de ruteadores que trabajan de acuerdo con RIP. Esta razón corresponde al principio básico de los protocolos DVA: usar información recibida a través de una tercera parte. El ruteador R2 ha pasado información a R1 relacionada con la disponibilidad de la red 201.36.14.0 sin ser capaz de confirmar su confiabilidad.

NOTA *Los loops o ciclos cerrados de enrutamiento no se generan cuando fallan las interfases o ruteadores. Si el ruteador R1 tuviera tiempo para pasar el mensaje acerca de la no disponibilidad de la red 201.36.14.0 antes de recibir información obsoleta desde R2, no habría loop de enrutamiento. Es necesario mencionar que en promedio, los loops o ciclos cerrados de enrutamiento surgen en no más de 50% de los casos posibles, aun sin tomar medidas especiales para prevenirlos. Los métodos para eliminar estos ciclos cerrados de enrutamiento se estudiarán en la siguiente sección.*

Métodos de eliminación de rutas inválidas en RIP

Aunque RIP no puede eliminar por completo estados transitorios en la red, cuando algunos ruteadores utilizan información obsoleta acerca de rutas no existentes, hay métodos que en la mayoría de los casos ayudan a resolver tales problemas.

La situación descrita en la sección anterior acerca de un ciclo cerrado de enrutamiento generado entre dos ruteadores vecinos podrá resolverse de manera confiable si se aplica un método que ha llegado a conocerse como **horizonte dividido**. Este método implica que la información de enrutamiento relacionada con alguna red almacenada en la tabla de ruteo de un ruteador específico nunca es enviada hacia el ruteador desde el cual se ha recibido (esto es el siguiente ruteador en la ruta actual).

Casi todos los ruteadores contemporáneos que funcionan de acuerdo con el protocolo RIP emplean la técnica de horizonte dividido. Si el ruteador R2 en el ejemplo descrito soporta la técnica del horizonte dividido, nunca pasará información obsoleta acerca de la red 201.36.14.0 hacia el ruteador R1 porque recibió esta información desde ese ruteador R1.

Sin embargo, la técnica de horizonte dividido no puede ayudar cuando los loops los crean más de dos ruteadores. Considérese con más detalle la situación que surge en la red mostrada en la figura 19.15 cuando el ruteador R1 pierde conectividad con la red 201.36.14.0. Supóngase que todos los ruteadores de esta red soportan la técnica del horizonte dividido. Los ruteadores R2 y R3 en esta situación no devolverán actos acerca de la red 201.36.14.0 con la métrica 2 a R1, pues este ruteador es el único desde el cual se recibió dicha información. Sin embargo, continuaría pasando información respecto a la disponibilidad de 201.36.14.0 con métrica 4 entre ellos, porque han recibido esta información desde una ruta combinada, no directamente desde el ruteador R1. Por ejemplo, el ruteador R2 recibió esta información desde la cadena R4-R3-R1. Por lo tanto, el ruteador R1 puede ser engañado otra vez hasta que cada ruteador en la cadena R3-R4-R2 descarte el registro acerca de la disponibilidad de la red 201.36.14.0.

Para prevenir la circulación del paquete en loops complejos después de fallas de enlace, existen otros dos métodos, conocidos como *actualizaciones disparadas* y *de mantenimiento.*

Con la **técnica de actualizaciones disparadas**, el ruteador, una vez que ha recibido los datos referentes al cambio de la métrica para una red específica, no espera la expiración del tiempo límite para actualizar la información de la tabla de ruteo. En vez de ello, transmite los datos acerca del cambio de ruta inmediatamente. En muchos casos, esta técnica puede evitar la transmisión de información obsoleta concerniente a la ruta fallida; sin embargo, sobrecarga la red con mensajes de control. Por consiguiente, las actualizaciones de disparo se llevan a cabo con cierto retraso. Debido a esto, es posible la situación en la que una actualización regular en algún ruteador tendrá lugar ligeramente antes de la llegada de la actualización de disparo desde el ruteador anterior. En consecuencia, este ruteador todavía tendrá tiempo para transmitir información obsoleta acerca de la ruta no existente dentro de la red.

La **técnica de mantenimiento** elimina tales situaciones. Este método implica incluir el tiempo límite de espera para recibir nueva información en la red que hace poco dejó de ser disponible. Este tiempo límite evita recibir información obsoleta relacionada con alguna ruta desde aquellos ruteadores localizados a cierta distancia del enlace fallido y que transmiten datos obsoletos acerca de su utilidad. Se supone que durante este periodo de dominación, dichos ruteadores descartarán esta ruta de sus tablas de ruteo, pues no recibirán ninguna información nueva respecto a ellas. En consecuencia, no propagarán información obsoleta atingente a la red.

19.3.3 Primera trayectoria más corta abierta

El protocolo de la primera trayectoria más corta abierta (OSPF) es una implementación contemporánea del algoritmo LSA. Se adoptó en 1991 y está caracterizado por muchas capacidades orientadas a usarlo en redes heterogéneas grandes.

Dos etapas de construcción de la tabla de ruteo

En OSPF, el proceso de construcción de la tabla de ruteo se divide en dos grandes etapas. En la primera etapa, cada ruteador construye la gráfica de los enlaces de red; los vértices de la gráfica son ruteadores y redes IP, mientras que los bordes de la gráfica son interfases de ruteador. Para conseguir esto, todos los ruteadores intercambian información con sus vecinos acerca de la gráfica de red que ellos tienen a su disposición hasta el caso actual. Este proceso es similar al de preparación de los vectores de distancia en RIP. Sin embargo, la información propagada es principalmente distinta, puesto que esta vez consiste en información relacionada con la topología de la red. El intercambio de mensajes de ruteadores se conoce como **anuncios de enlaces del ruteador**; además, cuando se transmite información topológica, los ruteadores no la modifican, como es el caso con los ruteadores RIP. Como resultado de la información topológica distribuida, todos los ruteadores tendrán información idéntica acerca de la gráfica de la red. Esta información se almacena en la **base de datos topológica** del ruteador, lo que también se conoce como **técnica de dominación de base de datos del estado del enlace**.

La segunda etapa consiste en determinar las rutas óptimas utilizando la gráfica recibida. Cada ruteador se considera a sí mismo el centro de la red y busca una ruta óptima para cada una de las redes conocidas. El problema de encontrar la trayectoria óptima de acuerdo con la gráfica de la red es bastante complejo y consume recursos. Para resolver este problema, OSPF implementa el algoritmo iterativo de Dijkstra. En cada una de las rutas encontradas utilizando este algoritmo, solamente se memoriza un paso: el hop hacia el ruteador siguiente de acuerdo con el principio del enrutamiento de un solo paso. Los datos referentes a este

paso se incluyen en la tabla de ruteo. Si varias rutas tienen la misma métrica hacia la red de destino, la tabla de ruteo almacenará los primeros pasos de todas estas rutas.

Anuncios de ruta HELLO

Después de construir una tabla de ruteo original, es necesario rastrear el estado de los enlaces de red e incorporar las correcciones en dicha tabla de ruteo. Los ruteadores OSPF no intercambian toda la información de la tabla de ruteo para controlar estados de enlace, como era el caso con los menos eficaces ruteadores RIP. En su lugar, transmiten breves mensajes especiales *HELLO*. Si el estado de la red no cambia, los ruteadores OSPF no corregirán sus tablas de ruteo ni enviarán anuncios de enlace a sus vecinos. Si el estado del enlace cambia, el ruteador enviará un nuevo anuncio a sus vecinos más cercanos, el cual se relacionará solamente con el enlace cuyo estado ha cambiado. Naturalmente, este enfoque tiene en cuenta un uso más económico del ancho de banda de la red. Una vez recibido un nuevo aviso acerca del cambio del estado del enlace, el ruteador reconstruye la gráfica de la red y repite el procedimiento de búsqueda de las rutas óptimas. Nótese que este último procedimiento no se relaciona con todas las rutas: sólo se recalculan las rutas afectadas por el cambio. Cuando se ha conseguido esto, el ruteador corrige su tabla de ruteo y puede transmitir el anuncio a sus vecinos más cercanos de manera simultánea excepto a aquel del cual se recibió este anuncio.

Cuando aparecen los enlaces con nuevos vecinos en la red, el ruteador obtiene esta información desde los nuevos mensajes *HELLO*. Aunque el tamaño de dichos mensajes es relativamente pequeño, todavía contienen información detallada acerca del ruteador que envió este mensaje así como de los datos referentes a sus vecinos más cercanos, lo cual permite identificar sin ambigüedades el ruteador. Los mensajes *HELLO* se envían cada 10 segundos para incrementar la velocidad de adaptación del ruteador a todos los cambios que tienen lugar en la red. El pequeño tamaño de estos mensajes permite una alta frecuencia de prueba de los vecinos de la red y los enlaces a ellos.

Métricas

Como regla, OSPF utiliza métricas que toman en cuenta el ancho de banda de la red; además, es posible utilizar otras dos métricas que consideran los requerimientos QoS especificados en el paquete IP: el retraso en la transmisión del paquete y la confiabilidad de entrega del paquete. Para cada una de las métricas usadas, OSPF construye una tabla de ruteo por separado. La selección de la tabla de ruteo requerida se lleva a cabo según el requerimiento QoS del paquete que llegó al ruteador (figura 19.16).

La estructura de una red así se muestra en la figura 19.17.

Los ruteadores están conectados a LAN y directamente a otro por medio de enlaces WAN de "punto a punto". En esos anuncios, OSPF distribuye información acerca de los siguientes tipos de enlaces: ruteador-ruteador y ruteador-red. Un ejemplo del primer tipo de enlace es el enlace "R3-R4", y la conexión "R4-195.46.17.0/24" es un ejemplo del segundo tipo de enlace. Adviértase que R3 y R4 también representan direcciones IP; no obstante, se utilizan identificadores simbólicos para distinguir estos vértices de la gráfica de las redes, para las cuales se ha preservado la notación estándar de las direcciones IP. Si los enlaces de punto a punto también son direcciones IP asignadas, llegarán a constituir vértices adicionales de la gráfica, como las LAN. La información acerca de la máscara de red se transmite con la dirección IP.

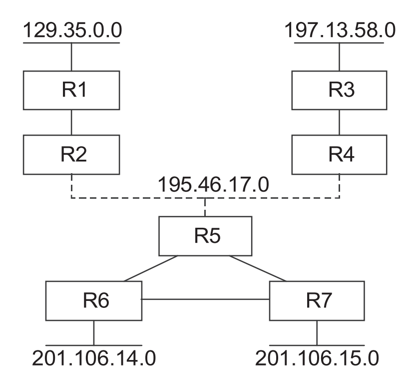


FIGURA 19.16 Fragmento de red.

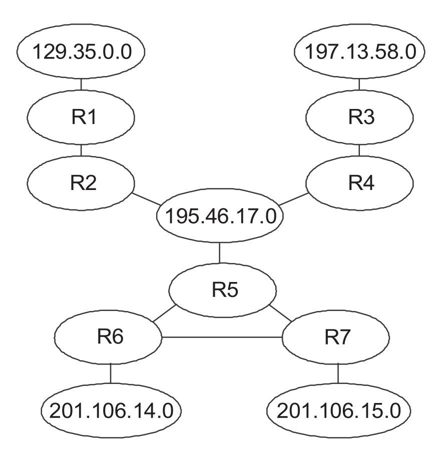


FIGURA 19.17 Gráfica de la red construida al utilizar el protocolo OSPF.

De modo similar a los ruteadores RIP, inmediatamente después de la inicialización, los ruteadores OSPF sólo tienen información acerca de los enlaces a redes conectados de manera directa y comienzan a distribuir esta información a sus vecinos. En paralelo con dicho proceso, envían mensajes *HELLO* a través de todas sus interfases de modo que el ruteador obtiene identificadores de sus vecinos más cercanos casi al instante. Esta información complementa la que conocía de su base de datos topológica de manera directa con información nueva. A continuación, la información topológica comienza a propagarse a través de la red de vecino en vecino y, después de algún tiempo, alcanza los ruteadores más distantes.

Cada enlace está caracterizado por una métrica. El protocolo OSPF soporta métricas que son estándar para muchos protocolos, como STA. Estos valores reflejan el rendimiento real de la red; para Ethernet, dicho valor es de 10 unidades; para Fast Ethernet, es de 1 unidad; para un canal T1, es de 65 unidades; para un canal de 56 Kbps, es de 1 785 unidades, y así sucesivamente. Cuando se utilizan enlaces de alta velocidad como Gigabit Ethernet o STM-16/64, un administrador debe determinar otra escala de velocidades mediante la especificación de una unidad de distancia convencional para el enlace de más alta velocidad.

Cuando se selecciona una ruta óptima en la gráfica, es necesario tener en cuenta la métrica relacionada con cada borde de la gráfica. Esta métrica se agrega a la de la trayectoria si se incluye un borde específico en esa trayectoria. Por ejemplo, en el caso descrito el ruteador R5 se encuentra conectado a los ruteadores R6 y R7 mediante enlaces T1, mientras que los ruteadores R6 y R7 están conectados entre sí por el enlace de 56 Kbps. En este caso, R7 de-

terminará una ruta óptima para la red 201.106.14.0 como una ruta combinada, que primero pasa a través del ruteador R5 y luego por R6, debido a que este ruteador tiene la métrica de ruta 65 + 65 = 130 unidades convencionales. La ruta directa a través de R6 no sería la óptima, pues la métrica de ruta sería de 1 785. Cuando se utilizan hops, la ruta que va a través de R6 se elegiría óptimamente, aun cuando no fuera la óptima.

El protocolo OSPF tiene en cuenta el almacenamiento de varias rutas hacia la misma red en la tabla de ruteo, a condición de que estas rutas estén caracterizadas por la misma métrica. Si existen tales registros de la tabla de ruteo, el ruteador enviará los paquetes a través de cada ruta de modo alternativo, para poner en práctica el modo de carga equilibrada.

Estabilidad OSPF

Cada registro en la base de datos topológica tiene su TTL, igual que los registros de enrutamiento de RIP. Cada registro acerca del estado del enlace tiene su cronómetro asociado que se utiliza para controlar el TTL del registro. Si cualquier registro de la base de datos topológica del ruteador recibido desde otro ruteador se torna obsoleto, el ruteador podrá solicitar otra copia de ese registro mediante el uso de un mensaje especial de *solicitud de estado del enlace* del protocolo OSPF. Para este mensaje, el ruteador tiene que recibir la respuesta de *actualización del estado del enlace* desde el ruteador que prueba directamente el enlace solicitado.

Cuando se inicializan los ruteadores y para una sincronización más confiable de las bases de datos topológicas, todos los registros de la base de datos se intercambian de manera periódica. Sin embargo, el periodo de intercambio para todos los registros de la base de datos es significativamente mayor que el periodo similar de los ruteadores RIP.

Debido a que la información acerca de un enlace específico se genera sólo por aquellos ruteadores que han probado el estado de ese enlace al enviar mensajes *HELLO* y otros ruteadores tan sólo retransmiten esta información sin modificaciones, no hay posibilidad de que aparezca información obsoleta en los ruteadores OSPF, en contraste con los ruteadores RIP. En los ruteadores OSPF, la información que resulta obsoleta se reemplaza rápidamente por información actualizada, debido a que después de que cambia el estado del enlace se genera de inmediato un nuevo mensaje.

En las redes OSPF, también puede haber periodos de funcionamiento u operación inestable. Por ejemplo, si falla el enlace, la información de este hecho no alcanzará a todos los ruteadores de inmediato. Si esta información no ha alcanzado un ruteador específico, éste continuará enviando los paquetes a la red de destino, porque considera que el enlace específico se halla disponible y es utilizable. Empero, estos periodos no duran mucho y los paquetes no se ubican en los "loops" o ciclos cerrados de ruta. Por el contrario, si es imposible transmitir el paquete por medio de un enlace no disponible, simplemente se descartará tal paquete.

La desventaja principal del protocolo OSPF es su complejidad, la cual requiere potencia de cómputo considerable, que se incrementa rápidamente con el crecimiento de la escala de la red (es decir, con un incremento en el número de redes, ruteadores y enlaces que los conectan). Para superar esta desventaja, se incluyó el concepto de *área* en el protocolo OSPF. No debe confundirse este concepto con el sistema autónomo de Internet. Los ruteadores que pertenecen a un área específica construyen la gráfica únicamente para esa área, lo que reduce el tamaño de la red. La información acerca de los enlaces no se transfiere entre áreas y los ruteadores de frontera intercambian sólo información relacionada con las direcciones de las redes existentes en cada una de las áreas, así como información referente a la distancia desde el ruteador de frontera a cada una de estas redes. Cuando se transmiten paquetes entre áreas, se selecciona uno de los ruteadores de frontera de un área específica. Como regla, dicho ruteador es aquel cuya distancia a la red requerida es la más corta.

19.3.4 Protocolo de compuerta de frontera

En la actualidad, el **protocolo de compuerta de frontera (o fronteriza) versión 4 (BGPv4)** es el protocolo principal utilizado para intercambiar información de ruteo entre los sistemas autónomos de Internet. BGP se diseñó para reemplazar a EGP,[5] el cual se empleaba cuando dicha red tenía solamente una troncal. Esta troncal era un sistema autónomo simple al cual se conectaban otros sistemas autónomos de acuerdo con una topología de árbol. Dado que esta estructura eliminaba toda posibilidad de loops entre los sistemas autónomos, EGP no tomó medidas adicionales para eliminar las posibilidades de loops de rutas.

> BGPv4 funciona con éxito con cualquier topología de enlaces entre sistemas autónomos, lo que corresponde al estado actual de Internet.

A continuación se explican los principios fundamentales del funcionamiento del BGP, para lo cual se usa el ejemplo de la figura 19.18.

En cualquiera de los tres sistemas autónomos (1 021, 363 o 520) existen varios ruteadores que desempeñan los papeles de compuertas exteriores. Estos ruteadores ejecutan el protocolo BGPv4, que utilizan para comunicarse entre sí. El ruteador interactúa con otros ruteadores de acuerdo con BGP solamente cuando el administrador de la red ha especificado de manera explícita que estos ruteadores son sus vecinos BGP en el curso de la configuración. Por ejemplo, el ruteador EG1 en el ejemplo en consideración interactuará con el ruteador EG2 de

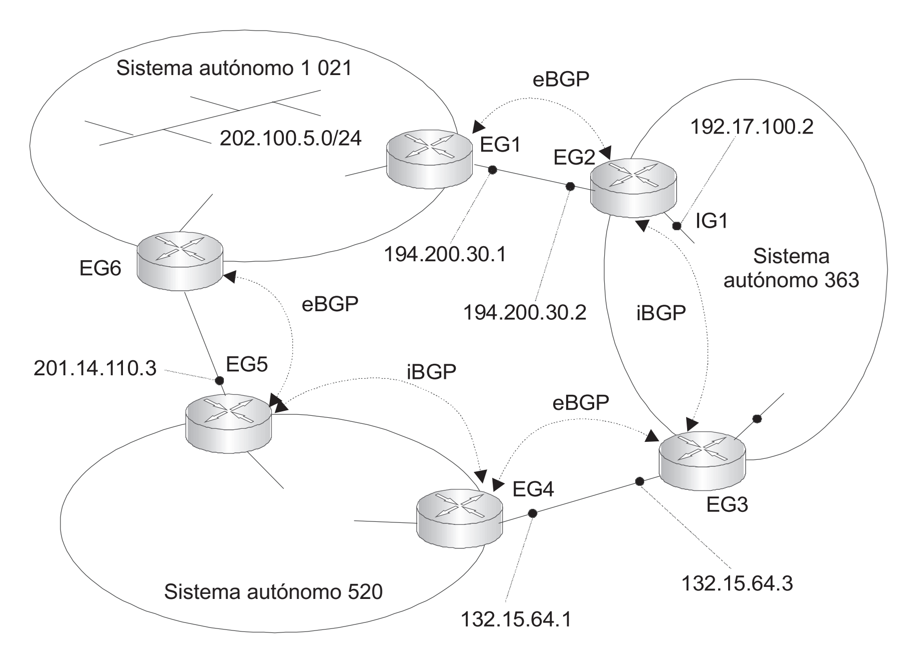


FIGURA 19.18 Búsqueda de una ruta entre sistemas autónomos al emplear BGP.

[5] EGP en este caso es el nombre del protocolo de ruteo específico. Recuérdese que la abreviatura EGP también sirve como el nombre de toda la clase de protocolos utilizados para ruteo entre sistemas autónomos. Esta coincidencia de nombres puede ser una fuente de confusión.

acuerdo con TCP, debido a que durante la configuración del ruteador EG1 el administrador especificó que el ruteador EG2 tiene la dirección 194.200.30.2, la cual se especificó para él como un vecino, no porque estos ruteadores se encuentren en conexión punto a punto. De manera similar, en el curso de la configuración del ruteador EG2, el ruteador EG1 con la dirección 194.200.30.1 se especificó como su vecino.

Dicho método de interacción es conveniente cuando los ruteadores intercambian información de ruta que pertenece a diferentes ISP. El administrador o administradores de un ISP específico pueden decidir con cuál sistema autónomo intercambiará tráfico este ISP y con cuáles sistemas no debe permitirse tal intercambio. Esta tarea se realiza al configurar la lista de vecinos para las compuertas exteriores del ISP. Los protocolos RIP y OSPF, diseñados para su uso dentro de un sistema autónomo, intercambian información de ruteo con todos los ruteadores localizados dentro de su alcance (utilizando una LAN o un enlace de punto a punto). Esto significa que la información acerca de todas las redes aparece en la tabla de ruteo de cada ruteador de manera que cada red esté al alcance de cualquier otra red. Para redes corporativas, esta situación es normal; para redes ISP, esto no es deseable. Debido a ello, BGP desempeña un papel especial aquí.

Para establecer una sesión con los vecinos especificados, los ruteadores BGP utilizan TCP (puerto 179). Cuando se establece una sesión BGP, pueden emplearse varios métodos de autenticación del ruteador con el fin de mejorar la seguridad de la operación del sistema autónomo.

El mensaje principal de BGP es el anuncio *Update* (*Actualizar*), cuyo uso del ruteador informa al ruteador del sistema autónomo vecino acerca del alcance al que se encuentran las redes con respecto a su propio sistema autónomo.

El nombre de este anuncio especifica que éstas son actualizaciones de disparo enviadas al vecino sólo cuando tienen lugar algunos cambios en el sistema autónomo. Tales cambios pueden relacionarse con la introducción de nuevas redes o rutas para las redes, o ser la desaparición de redes o rutas que ya existían.

Dentro de un mensaje simple de actualización o *Update* es posible anunciar una nueva ruta simple o revocar varias rutas que han dejado de existir. BGP interpreta una ruta como una secuencia de sistemas autónomos que tienen que pasarse para alcanzar la red especificada en la ruta. De manera más formal, la información acerca de la ruta BGT para la red especificada como `Network/Mask_length`, tiene el aspecto siguiente:

```
BGP Route = AS_Path; NextHop; Network/Mask_length;
```

AS_Path representa el conjunto de números del sistema autónomo, mientras que NextHop es la dirección IP del ruteador a través del cual es necesario pasar los paquetes a la red Network/Mask_length. Por ejemplo, si el ruteador EG1 necesita informar al ruteador EG2 que ha aparecido una nueva red (202.100.5.0/24) en el sistema autónomo AS1021, formará el mensaje siguiente:

```
AS1021; 194.200.30.1; 202.100.5.0/24,
```

Entonces, el ruteador lo pasa al ruteador EG2 del sistema autónomo AS363. Por supuesto, antes de hacerlo, el ruteador EG1 debe establecer una sesión BGP con el ruteador EG2.

El ruteador EG2, una vez que ha recibido un mensaje de *Update*, guarda la información acerca de la red 202.100.5.0/24 en su tabla de ruteo con el `NextHop 194.200.30.1` y marca que esta información se recibió desde BGP. El ruteador EG2 intercambia información de enrutamiento con ruteadores interiores de AS363, para lo cual emplea cualquier protocolo del grupo IGP; por ejemplo, éste puede ser mediante OSPF. Si el ruteador EG2 está configu-

rado para funcionar en el modo de redistribución de las rutas BGP a rutas OSPF, todos los ruteadores interiores de AS363 sabrán acerca de la existencia de la red 202.100.5.0/24 del anuncio OSPF del tipo exterior. Ahora, el ruteador EG2 especificará la dirección de su propia interfase interior como el NextHop; por ejemplo, éste puede ser 192.17.100.2 (para IG1).

Sin embargo, para propagar el anuncio relacionado con la red 202.100.5.0/24 en otros sistemas autónomos, como AS520, no puede utilizarse el protocolo OSPF. El ruteador EG3 conectado al ruteador EG4 del sistema autónomo AS520 debe usar BGP para generar mensajes *Update* del formato referido. Para llevar a cabo esta tarea, no puede emplear información relacionada con la red 202.100.5.0/24 recibida desde OSPF a través de una de sus interfases internas, pues tiene diferente formato y no contiene información respecto al número del sistema autónomo donde se localiza esta red.

Para resolver el problema, EG2 y EG3 también deben establecer una sesión utilizando BGP, aunque pertenezcan al mismo sistema autónomo. Este empleo de BGP se conoce como BGP interior en contraste con el uso principal, BGP exterior. Como resultado, el ruteador EG3 recibe la información requerida desde el ruteador EG2 y la pasa a su vecino externo, el ruteador EG4. Cuando se forma un nuevo mensaje *Update*, EG3 transforma el mensaje recibido desde el ruteador EG2 al agregar su propio sistema autónomo, AS520, a la lista de sistemas autónomos y reemplaza el valor `NextHop` recibido con la dirección de su propia interfase:

```
AS363, AS1021; 132.15.64.3; 202.100.5.0/24.
```

Los números de los sistemas autónomos permiten que el reciclaje de los mensajes *Update* sea eliminado. Por ejemplo, cuando el ruteador EG5 pasa el mensaje acerca de la red 202.100.5.0/24 hacia el ruteador EG6, este último no la utilizará, porque este mensaje tendrá el aspecto siguiente:

```
AS520, AS363, AS1021; 201.14.110.3; 202.100.5.0/24.
```

Como la lista de sistemas autónomos ya contiene el número del sistema autónomo local, es evidente que este mensaje se recicló.

En la actualidad BGT se utiliza para algo más que el intercambio de información de ruteo entre sistemas autónomos.

19.4 PROTOCOLO DE MENSAJE DE CONTROL DE INTERNET

PALABRAS CLAVE: protocolo de mensaje de control de Internet (ICMP, Internet Control Message Protocol), mejor esfuerzo, monitoreo de la red, mensajes de diagnóstico (error), consulta/respuesta de mensajes de información, formato de mensaje de error, destino inalcanzable, utilidad ping, protocolo de reenvío ("echo" o eco) y utilidad traceroute ("ruta de rastreo").

ICMP desempeña un papel auxiliar en la red. La especificación de este protocolo se describe en RFC 792.

Existen algunas situaciones en las cuales IP no puede entregar el paquete al host de destino. Por ejemplo, esto ocurrirá si el TTL del paquete ha expirado, si la ruta hacia la dirección de destino especificada se pierde de la tabla de ruteo, si el paquete no pasa la verificación por la suma verificadora, o si la compuerta no tiene suficiente espacio de búfer para pasar un paquete específico. Como se ha mencionado, IP funciona de acuerdo con el principio del **mejor esfuerzo**, lo cual significa que no toma ninguna medida especial para garantizar la entrega de los datos. Esta característica de IP es compensada por los protocolos de capa

superior tales como TCP en la capa de transporte o, para cierta extensión, por DNS en la capa de aplicación. Dichos protocolos asumen las responsabilidades de asegurar la confiabilidad. Para este propósito, emplean técnicas muy conocidas como la numeración de mensajes, el reconocimiento de entrega y la retransmisión de datos.

ICMP sirve como un suplemento para IP; sin embargo, la naturaleza de este suplemento es diferente de las capacidades para asegurar una transmisión confiable mediante protocolos de capa superior. ICMP no se diseñó para resolver los problemas que pueden surgir en el curso de la transmisión del paquete: si el paquete se ha perdido, ICMP no podrá retransmitirlo. El objetivo de ICMP es más simple. Este protocolo es el medio para informar al emisor acerca de cualquier "accidente" que ocurra a sus paquetes. Como IP envía el paquete y "olvida" todo acerca de su existencia, ICMP "rastrea" el proceso de envío del paquete a lo largo de la red; si el ruteador lo descarta, ICMP enviará el mensaje al host de origen y le informará de tal evento. De este modo, ICMP asegura una retroalimentación constante entre los paquetes enviados y el host emisor.

Por ejemplo, supóngase que al ejecutarse IP en un ruteador específico detecta que el paquete debe fragmentarse para enviarse a lo largo de la ruta, pero que el paquete tiene habilitada la bandera indicadora de no fragmentación *Don't Fragment* (DF). El módulo IP, una vez detectado que ya no puede pasar el paquete por la red, debe enviar el mensaje de *diagnóstico* ICMP al host de origen y luego descartar el paquete.

Aparte del diagnóstico, ICMP se utiliza para monitoreo de la red. Por ejemplo, las conocidas utilidades de diagnóstico destinadas para las redes IP, como `ping` y `tracert`, funcionan con mensajes ICMP. Si se emplean mensajes ICMP, una aplicación podrá determinar la ruta a lo largo de la cual se envían los datos, evaluar su utilidad, determinar el tiempo requerido para que los datos pasen hasta un host específico, solicitar el valor de máscara para una interfase específica de red y así sucesivamente.

Nótese que algunos paquetes pueden desaparecer de la red sin reconocimiento. En particular, ICMP no hace previsiones para pasar mensajes acerca de los problemas que surgen cuando se procesan paquetes IP que conducen mensajes de error ICMP. (No obstante, esta regla no es aplicable a solicitudes ICMP.) Los diseñadores de este protocolo utilizaron tal solución para evitar la generación de "tormentas" en las redes, cuando el número de mensajes de error se incrementa de manera explosiva. Por la misma razón, no se enviarán los mensajes ICMP si ocurre un error en el curso de la transmisión de cualquier fragmento excepto el primero, si el paquete perdido tiene una dirección IP de difusión, o si el paquete IP perdido fue encapsulado en la trama de la tecnología subyacente con una dirección de transmisión o difusión.

Debido a que un paquete IP contiene la dirección del emisor pero ninguna información de dirección acerca de los ruteadores de tránsito, los mensajes ICMP se envían únicamente a nodos terminales. Aquí, estos mensajes pueden ser procesados por el núcleo (kérnel) del sistema operativo, mediante protocolos de capa de transporte (o de aplicación) o por aplicaciones. Por otra parte, pueden ignorarse tales mensajes. El punto más importante es que el procesamiento de los mensajes ICMP no se incluye en la lista de responsabilidades de IP e ICMP.

19.4.1 Tipos de mensajes ICMP

Todos los mensajes ICMP ubican en una de las clases siguientes:

- Mensajes de diagnóstico (error).
- Mensajes de información tales como consulta y respuesta.

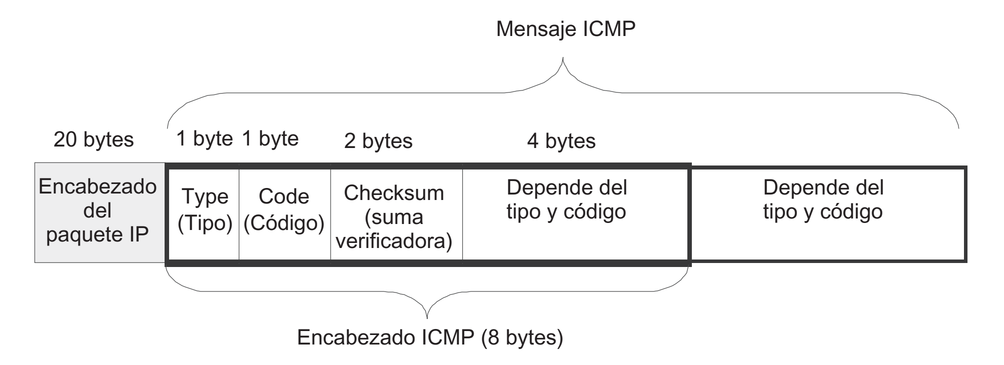


FIGURA 19.19 Formato y encapsulación de mensaje ICMP.

Un mensaje ICMP es encapsulado dentro del campo de datos de un paquete IP (figura 19.19). Un encabezado ICMP tiene 8 bytes de longitud y abarca los campos siguientes:

Tipo (Type) (1 byte): contiene el código para determinar el tipo de mensaje. La tabla 19.7 enumera los tipos más comunes de mensajes ICMP.

Código (Code) (1 byte): contiene el código que diferencia el tipo de error con más precisión.

Suma verificadora (Checksum) (2 bytes): es el campo de suma de verificación calculado para todo el mensaje ICMP.

El encabezado también incluye un campo que incluye 4 bytes. El contenido de este campo depende de los valores de los campos *Type* y *Code*. En los mensajes de consulta/respuesta, este campo contiene subcampos de 2 bytes *Identifier (identificador)* y *Sequence number (número*

TABLA 19.7 Posibles valores del campo Type (Tipo)

Valor	Tipo de mensaje
0	Respuesta de reenvío (eco)
3	Destino inalcanzable
4	Apagado de la fuente
5	Redirección
8	Solicitud de reenvío (eco)
11	Tiempo excedido para un datagrama
12	Problema de parámetro en un datagrama
13	Solicitud de marca de tiempo
14	Respuesta de marca de tiempo
17	Solicitud de máscara de dirección
18	Respuesta de máscara de dirección

de secuencia) (figura 19.20). Los números contenidos en estos subcampos son duplicados desde el mensaje de consulta hasta el mensaje de respuesta. El campo *Identifier* permite al host de destino determinar para qué aplicación se halla destinada esta respuesta, mientras que el campo *Sequence number* se aplica para relacionar la respuesta a una consulta específica (teniendo en cuenta que la misma aplicación puede producir varias consultas del mismo tipo). En mensajes de error, este campo no se utiliza y, en consecuencia, está llenado con ceros.

Mediante códigos de error pueden caracterizarse con más precisión errores de todo tipo. Por ejemplo, la tabla 19.8 contiene los códigos para el mensaje clasificado como de tipo 3: "destination unreachable" ("destino inalcanzable"). Dicha tabla enumera 15 razones que pueden especificarse en el mensaje de este tipo. La imposibilidad de alcanzar el host de destino puede ser causada, por ejemplo, por mal funcionamiento temporal de hardware, por una dirección de destino incorrecta, por la falta de un protocolo de capa de aplicación o por un puerto UDP/TCP abierto en el host de destino.

El formato del campo de datos ICMP también depende de los valores de los campos *Type* y *Code*. Para demostrar las diferencias en los formatos de los diversos tipos de mensaje, considérense los ejemplos siguientes:

- Solicitud/respuesta de reenvío (eco).
- Destino inalcanzable.

TABLA 19.8 Códigos que detallan la causa del error tipo 3: "destination unreachable"

Código	Causa
0	Red inalcanzable
1	Host inalcanzable
2	Protocolo inalcanzable
3	Puerto inalcanzable
4	Se requiere fragmentación, pero existe la indicación DF
5	Falla en la ruta de origen
6	Red de destino desconocida
7	Host de destino desconocido
8	Host de origen aislado
9	Red de destino prohibida por el administrador
10	Host de destino prohibido por el administrador
11	Red inalcanzable de acuerdo con el tipo de servicio (ToS)
12	Host inalcanzable de acuerdo con el ToS
13	Comunicación prohibida por el administrador mediante filtrado
14	Violación en la precedencia del host
15	Precedencia cortada en efecto

19.4.2 Formato del mensaje de solicitud/respuesta de reenvío o "eco": la utilidad Ping

La figura 19.20 ilustra el formato de los mensajes "echo request" ("solicitud de reenvío") y "echo reply" ("réplica de reenvío"), los cuales difieren entre sí solamente en el valor del campo *Type* (0 para la réplica y 1 para la solicitud). En el campo de datos de solicitud, el emisor coloca información, la cual recibe luego en la réplica desde el host de destino.

La solicitud de reenvío y la respuesta o réplica de reenvío, que en conjunto se denominan **protocolo de reenvío** ("**echo**"), son las herramientas más simples para monitorear la red. La computadora o ruteador envía una solicitud de reenvío a través de la interred, donde se especifica la dirección IP del host, aunque es necesario verificar la posibilidad de alcanzarlo. El host recibe la solicitud de reenvío, forma y envía una réplica de reenvío y devuelve el mensaje hacia el host que ha mandado la solicitud. Como las solicitudes y réplicas de reenvío pasan a través de la red en forma de paquetes IP, su entrega con éxito significa que todo el sistema de transporte de la interred funciona de manera normal.

La mayoría de los sistemas operativos utilizan la utilidad integrada ping, destinada para probar la posibilidad de alcanzar los hosts. Por lo regular, esta utilidad envía una serie de solicitudes de reenvío al host que se prueba y proporciona al usuario información estadística acerca de las réplicas de reenvío pérdidas y el tiempo promedio de reacción de la red a estas solicitudes.

```
# ping server1.citmgu.ru
Pinging  server1.citmgu.ru [193.107.2.200] with 64 bytes of data:

Reply from 193.107.2.200: bytes=64 time=256ms  TTL= 123
Reply from 193.107.2.200: bytes=64 time=310ms  TTL= 123
Reply from 193.107.2.200: bytes=64 time=260ms  TTL= 123
Reply from 193.107.2.200: bytes=64 time=146ms  TTL= 123
```

Del listado proporcionado aquí se sigue que se recibieron cuatro réplicas de reenvío en respuesta a las solicitudes de prueba enviadas al host server1.mgu.ru. La longitud de cada mensaje es de 64 bytes. La columna siguiente contiene los valores de RTT, los intervalos transcurridos desde que se envió la solicitud hasta que llega la réplica a su solicitud. Como se observa, la operación de la red no es estable, porque el valor RTT en la última línea es

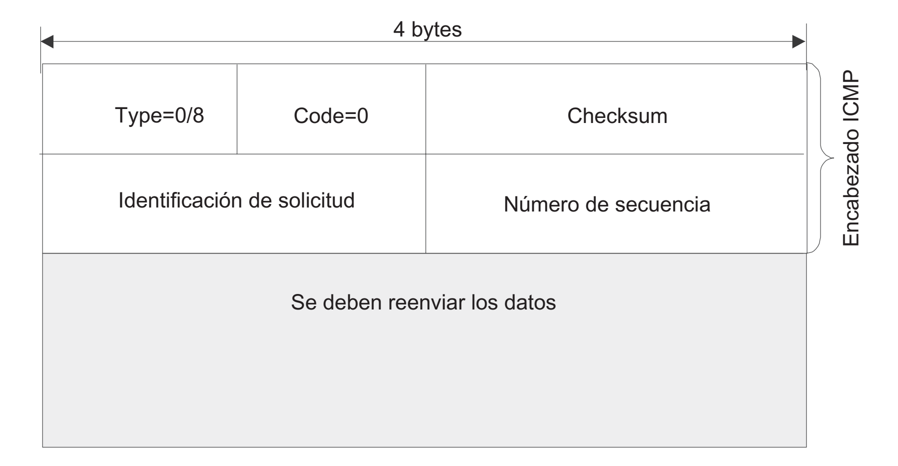


FIGURA 19.20 Formato de los mensajes ICMP *solicitud de reenvío/réplica de reenvío.*

más de dos veces más pequeño que el valor RTT de la segunda línea. El TTL restante para los paquetes que llegan se aprecia en la tercera columna.

Según la implementación específica de la utilidad ping y sus opciones de la línea de comandos, el comando de salida puede diferir del que se presenta aquí. Como regla, la utilidad ping tiene varias opciones de línea de comandos mediante cuyo uso es posible especificar el tamaño del campo de datos del mensaje, el valor inicial para los campos *TTL*, el número de intentos repetidos de transmisión del paquete y la configuración para la bandera *DF*.

Si no llegan respuestas o réplicas durante el tiempo límite especificado o si el ICMP responde con mensajes de error, ping mostrará mensajes de error apropiados en la pantalla.

19.4.3 Formato de mensaje de error: la utilidad Traceroute ("ruta de rastreo")

La figura 19.21 ilustra el formato del mensaje de error ICMP; en este ejemplo, es el mensaje "destination unreachable". Otros mensajes de error ICMP tienen el mismo formato y difieren entre sí únicamente en los valores de los campos *Type* y *Code*.

Si el ruteador no puede transmitir o entregar un paquete IP, enviará el mensaje de error "destination unreachable" al host que ha enviado este paquete. En dicho mensaje, el campo *Type* contiene el valor 3, mientras que el campo *Code* se llena con un número que va del 0 al 15, el cual especifica con más precisión la razón por la que no se entregó el paquete. Los 4 bytes que siguen a este campo son el campo de suma verificadora *Checksum*, bytes que no se utilizan y se llenan con ceros.

Además de la causa del error especificado en el encabezado ICMP, ICMP siempre llena su campo de datos con el encabezado IP y los primeros 8 bytes del campo de datos del paquete IP que ocasionó el error. Esta información permite al emisor determinar la causa del error con más precisión, pues todos los protocolos de la pila TCP/IP que usan paquetes IP para transmitir sus mensajes contienen la información más importante en los primeros 8 bytes de sus mensajes. En particular, éstos pueden ser los primeros 8 bytes del encabezado



FIGURA 19.21 Formato del mensaje de error ICMP "destination unreachable".

TCP o UDP, los cuales contienen la información que identifica la aplicación que ha enviado el paquete perdido. En consecuencia, los diseñadores de la aplicación pueden proporcionar herramientas integradas que se destinan para reaccionar a los mensajes ICMP en los paquetes que no podrían entregarse.

El host de destino o la red de destino puede ser inalcanzable debido a un mal funcionamiento temporal del hardware, a consecuencia de una dirección de destino incorrecta especificada por el emisor, o porque el ruteador no tiene información acerca de la ruta hacia la red de destino. La imposibilidad de alcanzar el protocolo, el puerto o ambos significa que el host de destino carece de la implementación de algún protocolo de capa de aplicación o que no tiene puertos abiertos UDP o TCP en el host de destino.

Como se vio en el ejemplo con la utilidad ping, los mensajes ICMP se utilizan con eficacia para el monitoreo de la red. En particular, los mensajes de error acerca de otro error, "time exceeded" ("tiempo excedido"), sirven como base para otra utilidad conocida: `traceroute` (en UNIX) o `tracert` (en Windows 2000). Esta utilidad permite rastrear la ruta hasta el host remoto y definir el RTT, la dirección IP y el nombre del dominio para cada ruteador de tránsito (a condición de que este nombre se haya registrado en la zona de búsqueda inversa de DNS). Esta información es útil para localizar el ruteador a través del cual la trayectoria del paquete hacia el host de destino llegó bruscamente a su fin.

Traceroute sigue la pista a la ruta al enviar paquetes IP normales con la dirección de destino mientras se investiga el final de la ruta. La idea del método de rastreo reside en que el TTL del primer paquete que se envía se establece a 1. Cuando el IP del primer ruteador recibe este paquete, disminuye el TTL en 1 de acuerdo con su algoritmo. El TTL obtiene un valor de cero y el ruteador descarta el paquete con el valor 0 del TTL y regresa el mensaje de "time exceeded" con el encabezado IP y los primeros 8 bytes del paquete perdido al host de origen.

Una vez recibido el mensaje ICMP informando al emisor por qué causa no se entregó el paquete, la utilidad `traceroute` memoriza la dirección del primer ruteador (recuperada desde el encabezado IP del paquete que conduce este mensaje ICMP). Después de ello, calcula el valor RTT para el primer ruteador. Posteriormente, `traceroute` envía el siguiente paquete IP con el valor TTL establecido a 2. Este paquete pasa con éxito el primer ruteador pero es descartado en el segundo, que inmediatamente envía el mismo mensaje ICMP de "time exceeded". La utilidad `traceroute` almacena la dirección IP y el TTL para el segundo ruteador, y así sucesivamente. La misma operación se realiza en cada ruteador siguiente a lo largo de la ruta hacia el host de destino.

Naturalmente, se ha considerado la operación de la utilidad `traceroute` de una forma simplificada. No obstante, incluso esta información es suficiente para evaluar la elegancia de la idea en que se basa.

El listado que se proporciona aquí muestra la salida típica de la utilidad `tracert` (Windows) en el curso de rastreo de **ds.internic.net** [198.49.45.29]:

```
 1  311 ms  290 ms  261 ms  144.206.192.100
 2  281 ms  300 ms  271 ms  194.85.73.5
 3  023 ms  290 ms  311 ms  moscow-m9-2-S5.relcom.eu.net [193.124.254.37]
 4  290 ms  261 ms  280 ms  MSK-M9-13.Relcom.EU.net [193.125.15.13]
 5  270 ms  281 ms  290 ms  MSK.RAIL-1-ATM0-155Mb.Relcom.EU.net [193.124.254.82]
 6  300 ms  311 ms  290 ms  SPB-RASCOM-1-E3-1-34Mb.Relcom.EU.net [193.124.254.78]
 7  311 ms  300 ms  300 ms  Hssi11-0.GW1.STK2.ALTER.NET [146.188.33.125]
 8  311 ms  330 ms  291 ms  421.ATM6-0-0.CR2.STK2.Alter.Net [146.188.5.73]
 9  360 ms  331 ms  330 ms  219.Hssi4-0.CR2.LND1.Alter.Net [146.188.2.213]
10  351 ms  330 ms  331 ms  412.Atm5-0.BR1.LND1.Alter.net [146.188.3.205]
11  420 ms  461 ms  420 ms  167.ATM8-0-0.CR1.ATL1.Alter.Net [137.39.69.182]
```

```
12  461 ms  441 ms  440 ms  311.ATM12-0-0.BR1.ATL1.Alter.Net [137.39.21.73]
13  451 ms  410 ms  431 ms  atlanta1-br1.bbnplanet.net [4.0.2.141]
14  420 ms  411 ms  410 ms  vienna1-br2.bbnplanet.net [4.0.3.154]
15  411 ms  430 ms  2514 ms  vienna1-nbr3.bbnplanet.net [4.0.3.150]
16  430 ms  421 ms  441 ms  vienna1-nbr2.bbnplanet.net [4.0.5.45]
17  431 ms  451 ms  420 ms  cambridge1-br1.bbnplanet.net [4.0.5.42]
18  450 ms  461 ms  441 ms  cambridge1-cr14.bbnplanet.net [4.0.3.94]
19  451 ms  461 ms  460 ms  attbcstoll.bbnplanet.net [206.34.99.38]
20  501 ms  460 ms  481 ms  shutdown.ds.internic.net [198.49.45.29]
Tracing complete.
```

La secuencia de líneas corresponde a la secuencia de ruteadores que forman la ruta hacia el host de destino. El primer número de cada línea es el número de hops hacia el ruteador apropiado. La utilidad `traceroute` prueba cada ruteador tres veces; por lo tanto, los tres números siguientes en cada línea son valores RTT calculados al enviar tres paquetes cuyos TTL han expirado en ese ruteador. Si la réplica desde un ruteador específico no llega durante el tiempo esperado, se pondrá un asterisco (*) en el lugar del tiempo.

Entonces, se especifican la dirección IP y el nombre de dominio (si está disponible) del ruteador. De esta lista, es claro que prácticamente todas las interfases del ruteador de ISP se han registrado en el servicio de DNS; las primeras, correspondientes a ruteadores locales, carecen de este registro.

Es necesario señalar otra vez que el tiempo especificado en cada línea no es el tiempo requerido para que el paquete pase entre los dos ruteadores vecinos. Mejor dicho, éste es el tiempo durante el cual el paquete pasa desde el origen al ruteador apropiado y de regreso nuevamente. Como la situación con la carrera de los ruteadores de Internet cambia de modo constante, el tiempo requerido para pasar a un ruteador específico no siempre crece a un ritmo constante. En ocasiones, puede cambiar de forma arbitraria.

RESUMEN

- En contraste con IP, cuya tarea principal consiste en asegurar la transmisión de datos entre interfases de red de la interred, el objetivo principal de TCP y UDP es la transmisión de datos entre procesos de aplicación que se ejecutan en diferentes nodos terminales de la red.
- La principal diferencia entre TCP y UDP es que aquél (TCP) lleva a cabo una tarea adicional: garantizar la entrega de mensajes confiable utilizando la interred, cuya totalidad de nodos usa un protocolo de datagrama IP no confiable para la transmisión de mensajes.
- UDP es un protocolo de datagrama que funciona de acuerdo con el principio del mejor esfuerzo, sin establecer una conexión lógica; además, UDP no garantiza la entrega de sus mensajes y, en consecuencia, no compensa la falta de confiabilidad de IP, que también es un protocolo de datagrama.
- Las colas del sistema a los puntos de acceso de los procesos de aplicación se llaman *puertos,* los cuales se identifican mediante números y sólo definen aplicaciones dentro de los límites de una computadora. Las aplicaciones que utilizan UDP tienen números denominados puertos UDP, mientras que las aplicaciones que dependen de TCP tienen puertos TCP.
- Si los procesos de aplicación son servicios públicos conocidos, como FTP, telnet, HTTP, TFTP o DNS, tienen números de puerto asignados centralmente. Los servicios que no se utilizan mucho y no tienen asignados números de puertos muy conocidos poseen

números de puerto asignados por el sistema operativo local. Tales números de puerto se denominan *dinámicos*.

- El socket de un proceso de aplicación es el siguiente par de sus parámetros: *dirección IP* y *número de puerto*.
- TCP resuelve el problema de asegurar el intercambio confiable de datos al establecer conexiones lógicas. Una conexión lógica se identifica unívocamente por medio de un par de sockets.
- Una conexión TCP es del tipo dúplex; se establece como resultado de negociación sobre el tamaño máximo de MTU, el volumen máximo de datos que se pueden transmitir sin recibir un reconocimiento, a partir del número de secuencia del byte desde el cual inicia el flujo de datos en una conexión específica. Cuando se crea una conexión, los sistemas operativos de ambos lados asignan un conjunto específico de recursos del sistema para aquélla. Estos recursos se requieren para organizar búferes, temporizadores o cronómetros y contadores.
- El procedimiento empleado por TCP/UDP cuando se reciben datos provenientes de varios servicios de aplicación se denomina *multiplexaje*. A su vez, el procedimiento inverso utilizado por TCP/UDP para distribuir los paquetes provenientes desde la capa de red entre el conjunto de servicios de capa superior se conoce como *demultiplexaje*. UDP implementa demultiplexaje con base en los switches, mientras que TCP lleva a cabo la misma tarea de acuerdo con conexiones.
- Para controlar el flujo dentro del marco de la conexión TCP, se utiliza una variante específica del algoritmo de ventana deslizante. El lado receptor transmite al emisor el tamaño de la ventana en bytes. Esta decisión se hace con apoyo en la velocidad a la que podrá procesar los datos entrantes; sin embargo, el emisor también puede controlar el tamaño de la ventana. Si el emisor nota que la operación del enlace de comunicaciones no es confiable, podrá reducir el tamaño de la ventana por iniciativa propia.
- Los protocolos de enrutamiento generan para cada ruteador tablas de ruteo coordinadas, es decir, aquellas que garantizarían la entrega segura del paquete a lo largo de una ruta racional desde la ruta de origen hasta la red de destino dentro de un número finito de pasos. Para este propósito, los ruteadores de red intercambian información especial acerca de la topología de la interred.
- El enrutamiento se clasifica en dos clases: estático y adaptativo (dinámico).
  - Durante el enrutamiento estático, todas las tablas de ruteo se componen e incluyen en cada ruteador de forma manual por el administrador de la red.
  - El enrutamiento adaptativo asegura la actualización automática de la tabla de ruteo después de cambiar la configuración de la red.
- Los protocolos de enrutamiento adaptativo están divididos en dos grupos, cada uno de los cuales se relaciona con cierto tipo de algoritmo:
  - En algoritmos de vector de distancia (DVA, por sus siglas en inglés), cada ruteador envía periódicamente mensajes de transmisión sobre la red, con los componentes representando las distancias desde este ruteador hacia todas las redes conocidas.
  - Los algoritmos de estados del enlace (LSA, por sus siglas en inglés) *proporcionan a cada ruteador información suficiente para elaborar una gráfica exacta de los enlaces de la red.*
- Los protocolos de enrutamiento de Internet se dividen en externos e internos. Los protocolos de compuerta exterior (EGP, por sus siglas en inglés) conducen información

de ruteo entre sistemas autónomos, mientras que los protocolos de compuerta interior (IGP, por sus siglas en inglés) se utilizan únicamente dentro de los límites de un sistema autónomo específico.

- RIP es el protocolo de enrutamiento más antiguo en las redes TCP/IP. A pesar de su simplicidad, ocasionada por el uso de un DVA, RIP se utiliza con éxito en redes pequeñas con no más de 15 ruteadores de tránsito.
- Los ruteadores RIP suelen seleccionar la ruta con base en la métrica más simple, el número de ruteadores de tránsito entre redes, o hops.
- En redes que utilizan RIP y tienen rutas cíclicas cerradas (con loops), puede haber periodos bastante largos de operación inestable, cuando los paquetes se hallan en ciclos cerrados o "loops" y no se entregan a su destino. Los ruteadores RIP proporcionan varias técnicas que en ocasiones reducen los periodos de inestabilidad. Estas técnicas incluyen horizonte dividido, dominación y actualizaciones disparadas.
- El protocolo OSPF fue diseñado para ruteo eficaz de los paquetes IP en redes grandes con topología compleja que incluyen ciclos cerrados o loops. Este algoritmo se basa en un LSA caracterizado por una alta estabilidad en contra de cambios de topología de la red.
- Cuando seleccionan una ruta, los ruteadores OSPF usan la métrica que tiene en cuenta el ancho de banda de la interred.
- El protocolo OSPF permite almacenar en la tabla de ruteo varias rutas hacia la misma red si éstas tienen métricas iguales. Ello facilita al ruteador funcionar en el estado de equilibrio de carga.
- OSPF es más complejo y requiere un gran poder computacional; por lo tanto, opera con mayor frecuencia en ruteadores de hardware poderosos.
- En la actualidad, el protocolo de compuerta fronteriza (BGP, por sus siglas en inglés) versión 4 es aquel para intercambio de información de ruteo entre sistemas autónomos de Internet. BGPv4 funciona con alta estabilidad y tiene cualquier topología de enlaces entre sistemas autónomos que corresponden a la estructura contemporánea de Internet.
- El protocolo de mensajes de control de interred (ICMP, por sus siglas en inglés) desempeña un papel subsidiario en la red y se utiliza para propósitos de diagnóstico y para monitoreo de redes. De este modo, los mensajes ICMP forman la base para utilidades tan conocidas para el monitoreo de redes IP como `ping` y `tracert`.

PREGUNTAS DE REPASO

1. ¿Cuándo prefieren los diseñadores de software utilizar UDP? y ¿cuándo prefieren confiar en TCP?
2. ¿Qué volumen de datos (con una precisión hasta de 1 byte) recibió durante la sesión TCP el emisor del segmento TCP cuyo encabezado contenía el valor 1 845 685 en el campo ACK, dado que el primer byte recibido tenía el número 50 046?
3. ¿Es posible enviar paquetes IP si el ruteador carece de una tabla de ruteo?
   a) No, esto es imposible.
   b) Sí, es posible a condición de que se utilice enrutamiento de origen.
   c) Sí, será posible si la ruta predeterminada se ha especificado en el ruteador.
4. ¿Es posible hacerlo sin protocolos de ruteo en la red?
5. ¿Cuáles son las desventajas de los protocolos de ruteo de vector de distancia?

a) Intenso tráfico extra en una red grande.
b) Las rutas seleccionadas no siempre se caracterizan por el mismo valor de métrica.
c) El proceso de coordinar tablas de ruteo toma mucho tiempo.

6. ¿Cuál es el principio principal de operación de los protocolos de enrutamiento basados en LSA?
7. ¿Cuál es la diferencia entre IGP y EGP?
8. ¿Qué métrica se utiliza en RIP?
9. ¿Por qué RIP considera inalcanzable la distancia de 16 hops?
   a) El campo asignado para almacenar el valor de la distancia tiene una longitud de 4 dígitos binarios.
   b) Las redes en las cuales opera el algoritmo RIP rara vez son grandes.
   c) RIP intenta asegurar un tiempo de convergencia aceptable de algoritmo.
10. ¿Qué métodos existen para acelerar la convergencia de RIP?
11. ¿Cuáles son las etapas principales de construcción para la tabla de ruteo utilizando OSPF?
12. ¿Cuál es el papel que desempeñan los mensajes *HELLO* en el protocolo OSPF?
   a) Establecen una conexión entre dos ruteadores.
   b) Verifican el estado de enlaces de comunicaciones y ruteadores vecinos.
   c) Conducen información que el protocolo OSPF opera en la red.
13. ¿Qué tipos de métricas soporta OSPF?
14. ¿Para qué propósitos se divide en áreas la red de ruteadores que soporta OSPF?
15. ¿Cuáles son las principales desventajas de OSPF?
16. ¿Por qué ya no se utiliza EGP en Internet?
17. ¿Cuál es el mecanismo que permite que BGP funcione en redes que tienen ciclos cerrados o loops entre sistemas autónomos?
18. ¿Qué parámetros cambia el ruteador BGP en el anuncio recibido desde algún sistema autónomo cuando lo pasa a otro sistema autónomo?
19. Si surge un problema con un paquete IP, ¿en qué casos es imposible enviar un mensaje de error ICMP?
20. ¿Cuál es el destino de un mensaje ICMP? y ¿qué módulo de software lo procesa?
21. ¿Cómo mejora un mensaje ICMP la confiabilidad de la transmisión de datos en una red IP?

PROBLEMAS

1. Encuentre un compañero y haga un modelo de una sesión TCP. Negocie el tamaño máximo del segmento, los tamaños iniciales de los búferes, los valores iniciales del SEQUENCE NUMBER (número de secuencia) y el tamaño de la ventana. Luego empiece a enviar "segmentos" entre sí de modo asincrónico. El rol de los "segmentos" puede ser jugado por tarjetas que contengan los valores de los campos clave (número del primer byte, tamaño del segmento que se envía, el ACKNOWLEDGMENT NUMBER (número de reconocimiento) y un nuevo valor del tamaño de la ventana). En ocasiones usted puede aparentar que ha perdido las cartas y actuar de acuerdo con la lógica de operación de TCP. No olvide marcar el tiempo para cada copia "enviada" del segmento con el fin de rastrear las llegadas de los reconocimientos. Este juego le ayudará a comprender mejor TCP. Haga las preguntas que quiera.

2. ¿Qué tiempo, en el peor de los casos, transcurrirá antes que las tablas de ruteo de la red mostrada en la figura 19.15 lleguen a un estado coordinado después de que el ruteador R1 pierda conexión con la red 201.36.14.0? Suponga que todos los ruteadores soportan el mecanismo del horizonte dividido.
3. Sugiera diversas variantes de la métrica que tenga en cuenta simultáneamente el ancho de banda, la confiabilidad y la latencia del enlace de comunicaciones.

20 CARACTERÍSTICAS AVANZADAS DE LOS RUTEADORES IP

DESCRIPCIÓN DEL CAPÍTULO

20.1 INTRODUCCIÓN

Las funciones principales de los operadores IP son la creación de tablas de ruteo y el envío de paquetes IP con base en estas tablas. Para llevar a cabo dichas funciones, el ruteador debe soportar el protocolo de Internet (IP) visto en el *capítulo 18,* además de los protocolos de enrutamiento considerados en el *capítulo 19*. Aparte de estas funciones básicas, los ruteadores IP contemporáneos soportan varias características avanzadas, lo que los hace dispositivos poderosos y flexibles de procesamiento de tráfico multifuncional. En este capítulo se estudiarán las capacidades avanzadas más importantes de los ruteadores contemporáneos utilizados con mayor frecuencia por los administradores de red.

Los ruteadores son dispositivos fronterizos que conectan una red de computadoras con el mundo exterior. Por lo tanto, sería natural delegarles varias funciones relacionadas con la *protección* de la red interna en contra de ataques desde el exterior. Los ruteadores IP llevan a cabo estas funciones con apego al filtrado de tráfico del usuario de acuerdo con varios atributos en los paquetes IP, como la dirección de origen, el tipo de protocolo encapsulado en el paquete y la aplicación que generó este tráfico. Tal funcionalidad evita el tráfico indeseable pendiente de la red protegida y reduce la probabilidad de ataques sobre los hosts localizados en esa red. La tecnología de *traducción de las direcciones de la red* (NAT, por sus siglas para *Network Address Translation*), que oculta de los usuarios externos las direcciones reales de los hosts pertenecientes a esta red, desempeña un papel importante en la protección de estos recursos de red internos.

El *soporte de QoS* es una propiedad relativamente nueva de las redes IP. Los ruteadores IP han soportado durante largo tiempo varios mecanismos de control de supresión y control de congestión; sin embargo, sólo hasta hace poco se diseñaron estándares para asegurar el soporte de QoS para redes IP, a finales de la década de 1990. Existen dos tipos de arquitectura de QoS para redes IP: *servicios integrados* (*IntServ, Integrated Services*) y *servicios diferenciados* (*Diff-Serv, Differentiated Services*). La primera arquitectura asegura la QoS para flujos individuales desde el origen hasta el destino, mientras que la segunda fue ideada para flujos agregados, que representan un pequeño número de clases de tráfico. En la actualidad, la tecnología IntServ se utiliza principalmente en la periferia de la red, en redes corporativas amplias y en redes de acceso. DiffServ ha comenzado a encontrar aplicación en troncales de red. Tal separación de las áreas de aplicaciones es evidente, pues asegurar la QoS para flujos individuales crea una carga adicional sobre el ruteador. Esta carga es proporcional al número de flujos a los que se da servicio. El troncal puede transmitir cientos de miles de flujos de usuario; por lo tanto, la implementación IntServ puede situar requerimientos demasiado elevados en la potencia de cómputo y la cantidad de memoria disponible para los ruteadores troncales.

En este capítulo se considera al final la estructura funcional de los ruteadores contemporáneos.

20.2 FILTRADO

PALABRAS CLAVE: filtrado de datos, filtrado de anuncios de ruteo, listas de acceso del ruteador, rechazo, permiso, lista de acceso estándar, comodines de origen, lista de acceso, palabras clave, ICMP, ping y protección.

Los protocolos de enrutamiento IP crean tablas de enrutamiento. Basados en éstas, cualquier host de la interred puede intercambiar información con cualquier otro host. Este principio

de redes de datagrama suele ser conveniente. Debido a ello, todo usuario de Internet puede tener acceso a cualquier sitio público.

Recuérdese que en las redes basadas en la técnica de circuito virtual es imposible organizar comunicaciones entre cualesquiera dos hosts sin establecer previamente un circuito virtual entre ellos.

Sin embargo, esta disponibilidad común de hosts y redes no siempre corresponde a las necesidades de sus propietarios. Por lo tanto, muchos ruteadores soportan características avanzadas, como filtrado de tráfico de usuario y anuncios del protocolo de enrutamiento. Estas capacidades controlan la disponibilidad de hosts con diferentes niveles de granularidad.

20.2.1 Filtrado de tráfico de usuario

El **filtrado** es un procesamiento no estándar de los paquetes IP mediante ruteadores, lo que da por resultado descartar paquetes específicos o modificar sus rutas.

El filtrado de tráfico del usuario implementado principalmente por los ruteadores es análogo a la función similar realizada por los conmutadores LAN (véase el *capítulo 15*).

El objetivo principal de filtrado reside en que no todos los paquetes IP que pasan a través del ruteador deben ser procesados de acuerdo con el procedimiento estándar descrito en el *capítulo 18*. En el procedimiento estándar, el tipo de procesamiento de paquete se elige con base en la información contenida sólo en el campo de la dirección de destino de un paquete IP.[1] Si esta dirección se encuentra en la tabla de ruteo, el paquete será transferido a la interfase de salida apropiada.

Las condiciones de filtrado del paquete establecidas en ruteadores por lo general encuentran un número considerablemente más grande de atributos que filtros semejantes implementados por los conmutadores LAN. Por ejemplo, aparte de la dirección IP de destino, la lista de tales atributos puede incluir lo siguiente:

- Direcciones IP de fuente y destino
- Direcciones MAC de fuente y destino
- Identificador de la interfase desde la cual se recibió el paquete
- Tipo de protocolo encapsulado en el paquete IP (por ejemplo, TCP, UDP, ICMP o OSPF)
- Número de puerto TCP/UDP (por ejemplo, tipo de protocolo de capa de aplicación)

Si el filtro está activado, el ruteador primero verificará si se satisfacen las condiciones especificadas en este filtro. Si el resultado de esta verificación es positivo, el ruteador llevará a cabo algunas operaciones no estándares para este paquete. Por ejemplo, el paquete puede ser descartado (abandonado), enviado al ruteador siguiente (que es diferente del especificado en la tabla de ruteo) o marcado como posible candidato para descartarlo si se presenta una

[1] Esta descripción se simplifica para destacar la principal característica del procedimiento estándar del envío de paquetes. En realidad, incluso el procedimiento estándar tiene en cuenta otros campos del paquete IPv, como *TTL*, el campo de datos (su tamaño), DF, la precedencia de *IP* y *ToS*. Si estos campos no requieren un procesamiento especial del paquete (como desechar el paquete si TTL ≤ 1), el ruteador comenzará el procedimiento de búsqueda de la tabla de ruteo.

congestión de la red. El procedimiento normal de pasar el paquete de acuerdo con los registros de la tabla de ruteo puede ser una de tales acciones posibles.

Considérense algunos ejemplos de filtros escritos utilizando el lenguaje de interfase de línea de comandos IOS de Cisco. Estos filtros, también denominados **listas de acceso**, se usan ampliamente para limitar el tráfico de usuario en ruteadores IP.

La **lista de acceso estándar** es el tipo más simple de filtro, que tiene en consideración sólo la dirección IP de origen.

La sintaxis general de una condición así tiene el aspecto siguiente:

```
access-list access-list-number {deny | permit}
      {source-address [source-wildcard] | any}
```

La lista de acceso estándar define dos acciones que pueden realizarse para el paquete que satisface la condición escrita por el filtro: `deny` (es decir, descartar el paquete) y `permit` (es decir, pasar el paquete para procesamiento estándar de acuerdo con la tabla de ruteo). Se elegirá la acción específica precisada en la lista de acceso estándar si la dirección IP de origen coincide con la dirección IP de origen indicada en la lista. La verificación se lleva a cabo de la misma manera que cuando se verifica una tabla de ruteo. Aquí, *`source-wildcard`* es el análogo de una máscara, pero de una forma ligeramente modificada. El cero binario en *`source-wildcard`* significa que este bit en la dirección del paquete que llega debe coincidir con la dirección especificada en la condición del filtro. El uno binario significa que no se requiere la coincidencia en esta posición. Si usted necesita especificar una condición para todas las direcciones de una subred específica, deberá utilizar el valor invertido de la máscara de esta subred. El parámetro *`any`* significa cualquier valor de la dirección: es una forma más breve y fácilmente comprensible de escribir el valor 255.255.255.255 en el campo *`source-wildcard`*.

Un ejemplo de la lista de acceso estándar es el que sigue:

```
access-list 1 deny   192.78.46.0   0.0.0.255
```

Aquí:

1: número de lista de acceso

`deny`: la acción que debe llevarse a cabo sobre el paquete que satisface la condición especificada en esta lista de acceso.

192.78.46.0: dirección de origen.

0.0.0.255: comodín (“wildcard”) de origen.

Este filtro bloquea la transmisión de los paquetes, cuyos tres bytes más significativos en las direcciones tienen los valores 192, 78 y 46.

La lista de acceso puede incluir varias condiciones. En este caso, abarca varias líneas a partir de la palabra clave `access-list`, la cual tiene el mismo valor de *`access-list-number`* que representa el identificador de lista. Por ejemplo, si usted necesita permitir que los paquetes originados desde el host 192.78.46.12 pasen al ruteador, denegando la transmisión de los paquetes desde los otros hosts pertenecientes a estas subredes, la lista de acceso tendrá el aspecto siguiente:

```
access-list 1 permit  192.78.46.12  0.0.0.0
access-list 1 deny    192.78.46.0   0.0.0.255
access-list 1 permit  any
```

Las condiciones de la lista de acceso se verifican una por una. Si cualquiera de ellas coincide, se llevará a cabo la acción `permit` o `deny` como se especifica en esta condición.

Después de ello, las otras condiciones especificadas en esta lista no se verifican. De manera predeterminada, al final de cada lista existe la siguiente condición implícita:

```
[access-list 1 deny any]
```

Por lo tanto, para evitar que esta lista interfiera con el procesamiento normal de los paquetes de otras redes, se escribe en ella la condición siguiente:

```
access-list 1 permit any
```

La lista de acceso puede aplicarse a cualquier interfase del ruteador en cualquier dirección. Si la lista se aplica con la palabra clave `in`, se aplicará al paquete entrante; si se emplea la palabra clave `out`, la condición se aplicará a los paquetes salientes. Por ejemplo, se puede aplicar `access-list 1` a alguna interfase para el tráfico entrante mediante el uso del comando siguiente:

```
access-group 1 in
```

Existen tipos más poderosos de listas de acceso para ruteadores Cisco, como las listas de acceso extendidas. El formato general de estas listas es el siguiente:

```
access-list access-list-number {deny|permit}
 {protocol|protocol key word}
 {source address [source-wildcard]] [source port] | any}
 [destination address [destination-wildcard]]   [destination port]
```

Si se emplea una lista de acceso extendida, se podrá evitar que el tráfico ftp que recibe solicitudes cliente al usar TCP con el número de puerto bien conocido 21 pase a la red interna de la compañía. Para lograr esto, es necesario incluir la condición siguiente en la lista de acceso:

```
access-list 102 deny  TCP any 21 any
```

Lo anterior debe aplicarse a la interfase del ruteador a la cual está conectada la red interna, con la palabra clave `out`.

Los administradores de redes de alcance empresarial suelen prohibir la posibilidad de hacer ping en hosts internos al emplear la condición siguiente:

```
access-list 101 deny ICMP any 192.78.46.8  0.0.0.0  eq 8
```

Como se ve en esa condición, la sintaxis de la lista de acceso (access-list) para ICMP es diferente de la sintaxis estándar utilizada para las listas de acceso extendidas. El parámetro 8 significa que está prohibido pasar mensajes ICMP del tipo 8, que corresponde a los mensajes de reenvío-solicitud usados por la utilidad `ping`.

El lenguaje de filtro del ruteador de software *Gated* empleado en muchas versiones UNIX es aún más flexible. Este lenguaje utiliza una sintaxis parecida a la del lenguaje C, que permite hacer construcciones lógicas más complejas mediante el uso de los operadores lógicos `if`, `then` y `else`.

Es necesario mencionar que el filtro del tráfico de usuario puede retardar de manera significativa la operación del ruteador, pues el procesamiento de cada paquete requiere verificar condiciones auxiliares.

Para evitar gastos importantes en el ruteador, "distrayéndolo" de este modo para realizar sus tareas principales, los filtros de ruteador no utilizan información acerca de la prehistoria de la sesión. Por complicada que sea la condición del filtro, contiene solamente los parámetros del paquete *actual* y no puede usar los parámetros de los paquetes procesados por el ruteador. Esta limitación es la principal diferencia entre ruteadores y muros de fuego,

sistemas de software especiales que emplean información acerca de la prehistoria de la sesión para llevar a cabo un mejor filtrado.

20.2.2 Filtrado de anuncios de ruteo

Para controlar la posibilidad de alcanzar redes y hosts específicos, es posible evitar la propagación de los anuncios de ruteo con el filtrado de tráfico de usuario.

Una medida así evita que los registros relacionados con ciertas redes aparezcan de modo automático en las tablas de ruteo. Este método requiere que el ruteador sea significativamente menos poderoso, pues los anuncios de ruteo llegan al ruteador pocas veces más que los paquetes del usuario.

Los ruteadores Cisco facilitan limitar la propagación de los anuncios de ruteo en una red específica al precisar su descripción mediante una lista de acceso estándar y luego al aplicarla a la interfase por medio de la palabra clave `distribute-list` (en lugar de la palabra clave `access-group`, como ocurría con el tráfico de usuario filtrado).

Por ejemplo, si un administrador de red quiere evitar que la información de las redes internas de la compañía 194.12.34.0/24 y 132.7.0.0/16 se propague a redes externas, será suficiente escribir la siguiente lista de acceso estándar:

```
access-list 2 deny 194.12.34.0 0.0.0.255
access-list 2 deny 132.7.0.0 0.0.255.255
access-list 2 permit any
```

Entonces, el administrador la aplicará a la interfase mediante el uso del comando siguiente:

```
distribute-list 2 out serial 1
```

20.3 QoS DE IP

PALABRAS CLAVE: servicios integrados, servicios diferenciados, clases de tráfico, RSVP, QoS, ISP, microrreflujo, flujo agregado, MPLS, algoritmo de cubeta de estafetas, algoritmo de detección aleatoria temprana (RED, Random Early Detection), RED ponderada (WRED, Weighted RED), mensaje PATH, mensaje RESV, reservación de recursos, descriptor del flujo, especificación de filtro, especificación de solicitud del receptor, especificación de tráfico de origen, direccionamiento expedito (EF, Expedited Forwarding) y direccionamiento asegurado (AF, Assured Forwarding).

Las tecnologías de la pila TCP/IP se crearon para un tráfico elástico, que es tolerante a retardos de paquetes y variaciones en el retardo de éstos. Por lo tanto, la atención de los diseñadores de TCP/IP estaba concentrada en asegurar la transmisión confiable del tráfico al utilizar TCP. No obstante, para eliminar sobrecargas y evitar la congestión en enlaces lentos, se construyeron gradualmente muchos mecanismos de QoS en ruteadores IP, incluidas colas de prioridad y ponderadas, política de tráfico y retroalimentación. Sin embargo, cada administrador de red era libre de usar estos mecanismos a su discreción sin ningún enfoque sistemático. Fue hasta mediados de la década de 1990 que comenzó la investigación en el campo del desarrollo de estándares de QoS para IP. Con base en estos estándares, fue posible crear un sistema de soporte de QoS dentro del marco de las interredes e incluso en Internet.

Como resultado de esa investigación, se diseñaron dos sistemas para la QoS de IP:

- Los *servicios integrados (IntServ, Integrated Services)* estaban orientados para proporcionar garantías de QoS para flujos de datos del usuario final. Por lo tanto, IntServ se utiliza principalmente en la periferia de la red.
- Los *servicios diferenciados (DiffServ, Differentiated Services)* se habían diseñado con el fin de hacer la misma labor para clases de tráfico. Por ello, se utilizan principalmente en los troncales.

Ambos sistemas emplean todos los elementos básicos del sistema de QoS basado en la reservación de recursos, es decir, ambos sistemas proporcionan los mecanismos siguientes:

- Condicionamiento de tráfico
- Señalización para coordinar el ruteador
- Reservación de la interfase y el ancho de banda del ruteador para flujos de clases de tráfico
- Colas ponderadas y de prioridad

Ninguna de esas tecnologías resuelve los problemas de ingeniería del tráfico, pues los paquetes aún se envían a lo largo de la trayectoria con la mejor métrica, que se elige mediante el protocolo de enrutamiento estándar sin tener en cuenta la carga real sobre los enlaces de comunicaciones.

20.3.1 Modelos de QoS de IntServ y DiffServ

El desarrollo de la tecnología IntServ lo inició IETF a principios de la década de 1990. Fue la primera área de desarrollo e investigación en la que el problema de asegurar la QoS para la red TCP/IP se resolvió con un enfoque sistemático. El modelo IntServ basg supone una comunicación integrada de los ruteadores de la red para asegurar la QoS requerida a lo largo de **la ruta del microflujo** entre nodos terminales de red.

Los recursos del ruteador (por ejemplo, ancho de banda de la interfase y tamaños de búfer) se distribuyen de acuerdo con los requerimientos de QoS de varias aplicaciones dentro de los límites permitidos por la política de QoS para la red dada. A su vez, las solicitudes de la aplicación de QoS se propagan a través de la red al usar el protocolo de señalización RSVP, que permite reservaciones tanto para los flujos entre dos nodos terminales (por ejemplo, direcciones de destino unidirigidas) como para flujos recibidos por varios nodos terminales (por ejemplo, direcciones de destino multidirigidas).

Sin embargo, este sistema armonioso para asegurar la QoS tiene numerosos oponentes, sobre todo entre los ISP. Esto se debe a que la implementación de IntServ exige que los ruteadores troncales de los ISP funcionen con la información del estado de decenas de miles de microflujos que pasan a través de las redes del ISP. Esas carreras no tradicionales sobre los ruteadores requieren volver a diseñar sus arquitecturas, lo cual incrementa en gran medida el costo de las redes IP y sus servicios.

De lo anterior se infiere que, a finales de la década de 1990, se diseñó otra tecnología de QoS de IP, conocida como **DiffServ**. En sus inicios, esa tecnología tenía como finalidad su aplicación dentro de los límites de la red ISP, pero excluía nodos terminales que generan microflujos fuera de consideración. Para la tecnología DiffServ, el soporte de QoS comienza en el ruteador de orilla de la red ISP, al cual llega un gran número de microflujos desde la red del usuario. Cada ruteador fronterizo de DiffServ clasifica y etiqueta el tráfico entrante, al cual divide en un pequeño número de clases, que por lo regular no excede de 3 a 4 (con un máximo de 8). Luego, cada ruteador de red sirve las clases de tráfico con base en esta diferenciación, de acuerdo con el etiquetado realizado y asigna cierta cantidad de recursos

para cada clase. Los recursos en los ruteadores se reservan de manera estática. Con más frecuencia, esta tarea la llevará a cabo manualmente un administrador de red. El papel del protocolo de señalización se lleva a cabo mediante las etiquetas que establecen que un paquete específico pertenece a una clase determinada.

La responsabilidad del servicio coordinado del tráfico por los ruteadores de la red es delegado al administrador, porque él decide el ancho de banda y la cantidad de espacio de búfer asignado para cada clase de tráfico en cada interfase de cada ruteador.

El modelo DiffServ reduce significativamente la carga sobre los ruteadores ISP, pues requiere que la información del estado se almacene sólo para un pequeño número de clases de tráfico. Además, este modelo es conveniente para los ISP debido a que les permite organizar el soporte de QoS de forma autónoma dentro de los límites de las redes propiedad de esos ISP. Sin embargo, se debe pagar por tener dichas ventajas. En este caso, las ventajas se obtienen a expensas del soporte de QoS de terminal a terminal. Incluso si cada ISP incrementa DiffServ en su red, se fragmentará todo el patrón, pues los administradores individuales son responsables de cada fragmento. La coordinación de los parámetros de reservación permanece como un procedimiento exclusivamente subjetivo, lo cual no es soportado por cualquier protocolo.

A pesar de la gran atención depositada últimamente en DiffServ como una herramienta simple que puede utilizarse para asegurar la QoS de Internet incrementada sin gastos significativos, existen puntos de vista alternativos. Por ejemplo, el doctor Lawrence G. Roberts, uno de los fundadores de Internet, ha expresado una opinión extremadamente negativa acerca de los intentos por resolver los problemas de QoS de dicha red en una forma simplificada. La investigación del uso combinado de las tecnologías IntServ y DiffServ también se encuentra en progreso. En estos modelos, cada tecnología funciona en su área de aplicación: IntServ en redes de acceso, donde el número de microflujos es relativamente pequeño, y DiffServ en redes troncales. Otro componente que complementa a DiffServ es la tecnología de conmutación de etiquetas multiprotocolo (MPLS) que permite resolver el problema de ingeniería del tráfico en redes IP. Esta tecnología se verá con más detalle en la *parte V*, cuyo objetivo principal se centra en las tecnologías WAN, pues apareció al combinar IP con una tecnología WAN tan conocida como ATM. En consecuencia, es mucho más fácil estudiarla después de aprender lo relacionado con ATM.

IntServ y DiffServ (RFC 3290) confían en los mismos mecanismos básicos de QoS. En particular, en ruteadores IP, el algoritmo de cubeta de estafetas se aplica para la política de tráfico. Aparte de ello, para evitar la congestión cuando se utiliza TCP, los ruteadores emplean tradicionalmente un mecanismo de retroalimentación específico, denominado *detección aleatoria temprana* (RED, por sus siglas en inglés).

20.3.2 Algoritmo de cubeta de estafetas

El a*lgoritmo de cubeta de estafetas está basado en una comparación del flujo del paquete con algún flujo de referencia que tiene una velocidad promedio predefinida*. Este flujo de referencia se representa por señales o estafetas suministradas a una de las entradas del servidor, que decide cuándo enviar los paquetes que llegan a la segunda entrada (figura 20.1).

En este caso, la "señal" o "estafeta" es interpretada como algún objeto abstracto que es el portador de alguna "parte" de información utilizada para construir el modelo del servicio de tráfico. El generador de estafeta se dirige de manera periódica a la siguiente estafeta den-

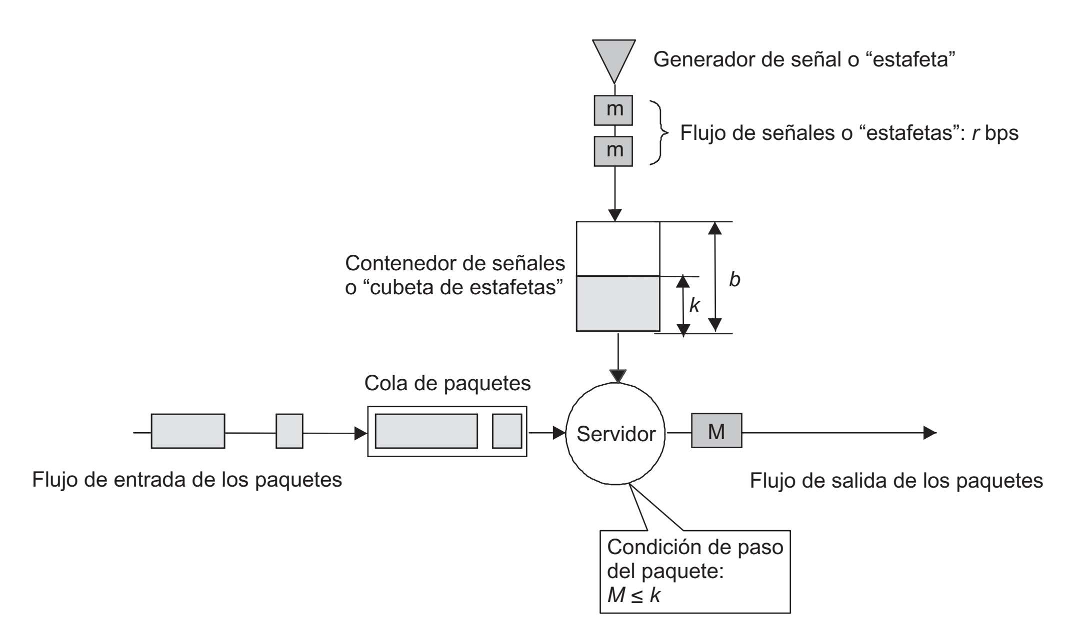


FIGURA 20.1 Algoritmo de cubeta de estafetas.

tro del contenedor o “cubeta” que tiene un volumen limitado de *b* bytes. Todas las estafetas tienen el mismo tamaño, igual a *m* bytes, y se generan de tal modo que se llegue a la cubeta a la velocidad de *r* bytes por segundo. Evidentemente, esta velocidad es igual a $r = 8m/w$. La tasa o velocidad *r* es la máxima velocidad promedio para el tráfico que se forma. El tamaño de la cubeta corresponde a la máxima magnitud de la ráfaga del flujo de paquetes. Si la cubeta se llena con estafetas (es decir, la cantidad total de estafetas en la cubeta es igual a *b*), se detendrá temporalmente el suministro de ellas. En realidad, la cubeta de estafetas representa el contador que es incrementado en *m* cada *w* segundos.

¿Cuándo se debe usar el algoritmo de cubeta de estafetas? El perfil del tráfico está definido por la **velocidad** *r* y el **tamaño de ráfaga** *b*.

La comparación de los flujos de referencia y real la realiza el servidor, el cual representa un dispositivo abstracto con dos entradas. La entrada 1 está conectada a la cola de paquetes, y la entrada 2 a la cubeta de estafetas. El servidor también tiene una salida, a la cual pasa los paquetes desde la cola de entrada. La entrada 1 del servidor modela la interfase de entrada del ruteador, mientras que la salida simula la interfase de salida del ruteador.

> El paquete de la cola es enviado por el servidor solamente si a su llegada a él la cubeta está llena con estafetas hasta un nivel no menor que *M* bytes, donde *M* es el tamaño del paquete.

Si se satisface esa condición, el paquete se enviará a la salida del servidor y las estafetas de la cantidad total de *M* bytes (con los *m* bytes de precisión) se eliminarán de la cubeta. Si la cubeta no se ha llenado al nivel suficiente, se procesará el paquete con uno de los siguientes métodos no estándares según el objetivo de uso del algoritmo.

- Si el algoritmo de cubeta de estafetas se utiliza para moldear el tráfico, el paquete simplemente se diferirá en la cola durante un tiempo adicional, durante el cual espera a que el número suficiente de estafetas llene la cubeta. De este modo, es posible conseguir la uniformidad del tráfico: incluso cuando un gran número de paquetes ha llegado al sistema

como resultado de una ráfaga, los paquetes abandonan la cola de manera más uniforme a la velocidad especificada por el generador de estafetas.

- Si el algoritmo de cubeta de estafetas se emplea para perfilar el tráfico, se descartará el paquete como uno que no corresponde al perfil. Otra solución más relajada es remarcar el paquete de tal forma que disminuya su estado en el curso de servicios adicionales. Por ejemplo, el paquete puede ser marcado mediante un atributo especial elegible para eliminación. En este caso, los ruteadores descartarán tales paquetes en primer lugar si surge una congestión. Cuando se utiliza DiffServ, el paquete puede ser desplazado a otra clase de tráfico que tenga una prioridad inferior y se le proporciona una QoS inferior.

NOTA *El algoritmo tolera ráfagas de tráfico dentro de ciertos límites. Supóngase que el ancho de banda de la interfase, cuya velocidad está limitada por el algoritmo de cubeta de estafetas, es igual a R. Entonces es posible demostrar que para cualquier intervalo de tiempo t, la velocidad promedio del flujo del servidor es igual al mínimo de los dos valores: R y r + b/t. Si los valores de t son grandes, la velocidad del flujo de salida tenderá a r, lo cual sirve como evidencia de que el algoritmo asegura la velocidad promedio deseada. Al mismo tiempo, durante un pequeño intervalo t (cuando r + b/t > R) el paquete puede dejar el servidor a la máxima velocidad posible para la interfase y crear así una ráfaga. Esta situación tiene lugar cuando los paquetes no llegan al servidor durante algún tiempo, de modo que la cubeta se llena con estafetas (es decir, durante el tiempo mayor que b/r). Si llega una gran secuencia retrasada de paquetes al servidor, éstos se pasarán a la salida a la velocidad de la interfase de salida R, también uno por uno sin intervalos.*

El tiempo máximo de tal ráfaga es b/(R – r) segundos, después de los cuales se requerirá una pausa para llenar la cubeta vacía. El tamaño de la ráfaga es Rb/(R – r) bytes. Con base en la fórmula proporcionada, puede observarse que el algoritmo de cubeta de estafetas comenzará a funcionar de manera inadecuada si la velocidad promedio r se elige cerca del ancho de banda de la interfase de salida. En este caso, la ráfaga puede continuar durante largo tiempo, lo que degrada la operación de dicho algoritmo.

20.3.3 Detección aleatoria temprana

La técnica RED (Random Early Detection) es el mecanismo de perfilación del tráfico TCP diseñado por la comunidad de Internet para evitar la congestión de los troncales de esta red.

El objetivo principal de RED es evitar la congestión grave de la red. RED funciona con el confiable protocolo de transporte TCP y usa el algoritmo de relación TCP en pérdidas de paquetes. Esta relación consiste en que la fuente del tráfico reduce la transmisión de los paquetes en la red. RED utiliza esta propiedad como una retroalimentación implícita para notificar al origen que genera los datos con demasiada intensidad.

El algoritmo RED utiliza dos umbrales configuradores del nivel de congestión (figura 20.2). Cuando el nivel de congestión es inferior al primer umbral, `LowThreshold`, los paquetes no se descartan. Cuando el nivel de congestión se ubica entre dos valores de umbral, se descartan los paquetes con la probabilidad linealmente creciente dentro del intervalo de 0 al valor configurable MaxDropProbability. El último valor se alcanza exactamente cuando se llega al segundo umbral, TopThreshold (figura 20.2). Cuando la congestión excede el segundo umbral, los paquetes se descartan con la probabilidad de 100 por ciento.

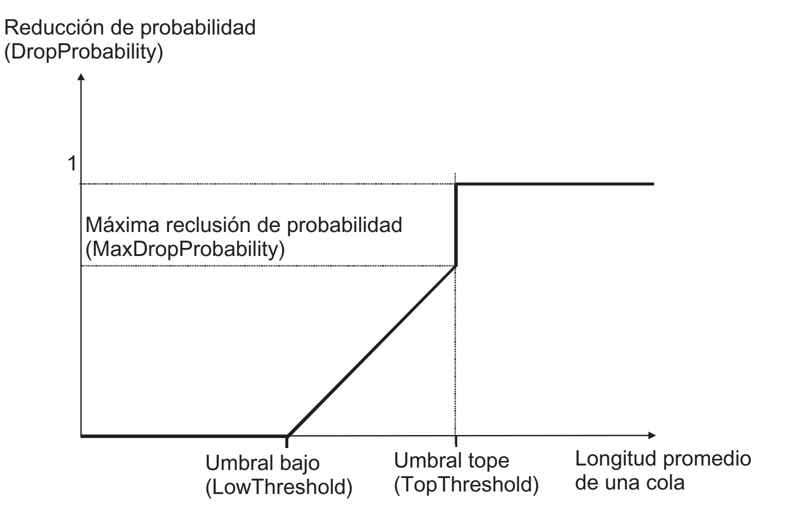


FIGURA 20.2 Probabilidad de descarte de paquetes en los que se utiliza el algoritmo RED.

La longitud promedio de la cola de paquetes pertenecientes a una sesión TCP específica se utiliza como la medida de la congestión.

NOTA *Obsérvese que para tráfico UDP, no es aplicable el mecanismo RED, pues UDP es un protocolo sin conexión que no establece conexiones lógicas ni advierte de pérdidas de paquetes.*

Cuando es necesario asegurar varios parámetros de retroalimentación para diferentes clases de tráfico, se emplea el *algoritmo RED ponderado* (*WRED, Weighted RED*). Esta variante de RED permite que se especifiquen valores por separado de `LowThreshold`, `TopThreshold` y `DropProbability` para cada clase de tráfico. Por lo regular, el mecanismo WRED se utiliza con WFQ y se asegura la entrega confiable del tráfico TCP con una proporción garantizada.

20.3.4 Marco de servicios integrados y RSVP

IntServ se basa en la reservación de recursos de ruteador a lo largo de la trayectoria del flujo de datos de un nodo terminal a otro. Para ser más precisos, los sistemas terminales, reservados en este caso, no son computadoras. En su lugar, éstas son aplicaciones que se ejecutan en los nodos terminales (figura 20.3). La aplicación debe utilizar la API apropiada con el fin de pasar la solicitud de reserva de recursos para un flujo específico. Esta reservación es unidireccional. Por lo tanto, si es necesario garantizar la QoS para intercambio de datos bidireccional, se deben llevar a cabo dos operaciones de reservación.

La reservación en el modelo IntServ se realiza mediante el **protocolo de reservación** (RSVP), que es de señalización, semejante en muchos aspectos a los protocolos de señalización empleados en **redes telefónicas**.

Sin embargo, las características específicas de las redes de conmutación de paquetes de datagrama afectan naturalmente su operación. De este modo, los parámetros de conmutación en redes IP no representan el atributo de reservación, porque los ruteadores pasarán paquetes IP con base en la tabla de ruteador con o sin reservación.

La reservación de los recursos de red requeridos al usar RSVP se lleva a cabo de la manera descrita a continuación y todos los tipos de mensajes mencionados en esta descripción se resumen en la tabla 20.1:

1. La fuente de los datos (computadora C1 en la figura 20.3) envía el mensaje especial PATH a la dirección única o de grupo (la figura 20.3 ilustra este último caso), donde especifica los parámetros recomendados para la recepción de alta calidad de su tráfico: umbrales superior e inferior del ancho de banda, retardo y variación del retardo. Estos parámetros de tráfico están contenidos en la *especificación de tráfico* (TSpec). El mensaje PATH se pasa mediante los ruteadores de red hacia el destino (o destinos) de acuerdo con las tablas de ruteo obtenidas al emplear cualquier protocolo de enrutamiento (por ejemplo, OSPF). Para especificar los parámetros de tráfico, se utilizan los parámetros del algoritmo de cubeta de estafetas (por ejemplo, velocidad promedio y profundidad de la cubeta). Además, pueden especificarse de manera adicional la máxima velocidad permitida y los límites de las dimensiones de los paquetes de este flujo.
2. Cada ruteador que soporta RSVP, una vez que ha recibido los mensajes PATH, registra el "estado de trayectoria", el cual incluye la dirección anterior del origen del mensaje PATH: el paso siguiente en la dirección inversa (es decir, llevando hacia la fuente o el origen). Esto es necesario para asegurar que la respuesta desde el receptor sigue la misma trayectoria que el mensaje PATH.
3. Después de recibir el mensaje, el receptor (una aplicación que se ejecuta en el nodo de destinos) envía la solicitud de reservación de recursos del mensaje RESV hacia el ruteador desde el cual ha recibido este mensaje. El mensaje RESV es una solicitud para reservación de recursos. La figura 20.3 muestra dos receptores: las computadoras C2 y C3. Además de la información TSpec, el mensaje RESV incluye la *especificación de la solicitud* (RSpec), en la cual se determinan los parámetros de QoS requeridos para el receptor y

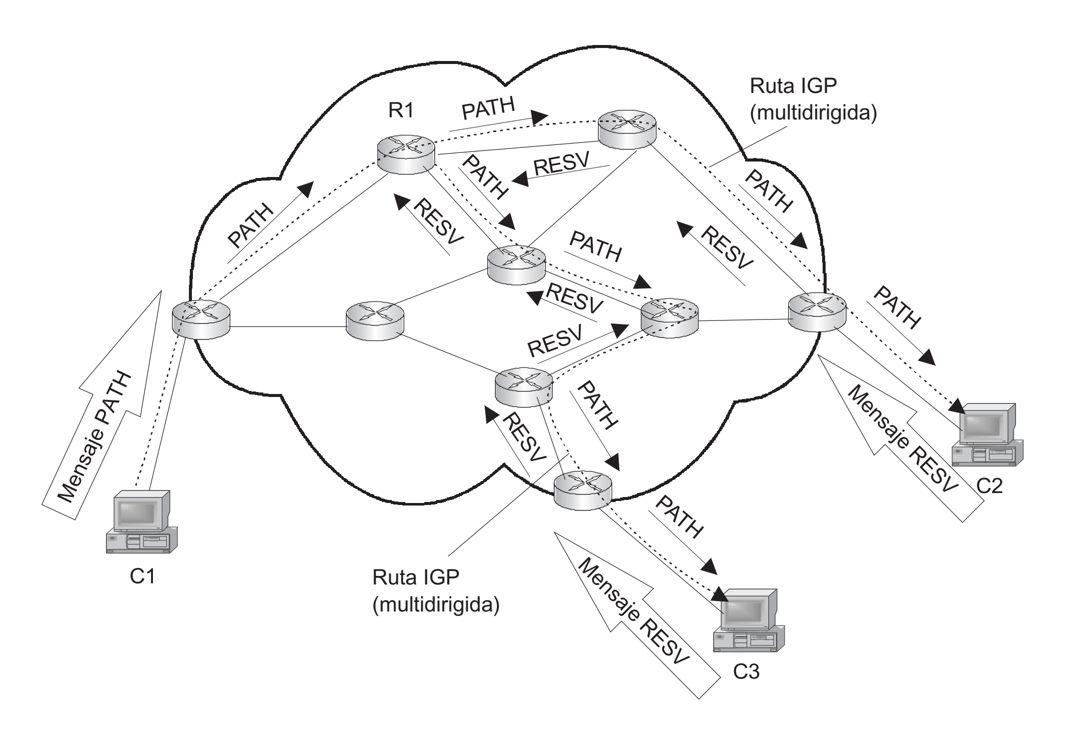


FIGURA 20.3 Reservación de recursos en los que se utiliza RSVP

TABLA 20.1 Mensajes RSVP

Tipos de mensaje	Contenido
Mensaje PATH desde el origen hasta el destino	Especificación del tráfico del origen.
Especificación del tráfico de origen	Parámetros recomendados para recepción de tráfico de calidad: límites superiores de inferior del ancho de banda, retardos y variaciones de retardo, parámetros del algoritmo de la cubeta de estafetas (velocidad promedio y profundidad de la cubeta). Adicionalmente, es posible especificar la velocidad máxima permitida y los tamaños del umbral de los paquetes de flujo.
Especificación de filtro	Especifica a qué paquetes de la sección debe aplicarse esta reservación (por ejemplo, de acuerdo con el tipo de protocolo de transporte y el número de puerto).
Especificación de solicitud del receptor	Parámetros de QoS requeridos para el receptor.
Descriptor del flujo	Especificación de filtro + especificación de solicitud del receptor.
Mensaje RESV: solicitud para reservación de recursos	Especificación del tráfico de origen o de la fuente + descriptor del flujo.

la *especificación de filtrado* (filterspec), que define a cuáles paquetes de la sesión debería aplicarse esta reservación (por ejemplo, mediante el tipo de protocolo de transporte y el número de puerto). La combinación de RSpec y filterspec es el *descriptor de flujo*, que el ruteador utiliza para identificar cada reservación de recursos. Los parámetros de QoS solicitados en la especificación RSpec pueden diferir de los señalados en TSpec. Por ejemplo, si el receptor ha decidido no recibir todos los paquetes enviados por la fuente u origen pero recibir selectivamente sólo parte de ellos (lo cual puede especificarse al usar la especificación de filtros), necesitará menos ancho de banda.

4. Cuando cualquier ruteador que soporta RSVP a lo largo de la ruta recibe el mensaje RESV, lo transfiere en una dirección hacia arriba y utiliza dos procesos para determinar la aceptabilidad de los parámetros de reservación especificados en esta solicitud. Al emplear el mecanismo de control de admisión, la verificación del ruteador tiene los recursos requeridos para soportar el nivel de QoS solicitado. El proceso de control de política se utiliza para verificar si el usuario tiene derecho a reservar los recursos. Si no se puede satisfacer la solicitud por una falta de recursos o debido a un error de autorización, el ruteador devolverá un mensaje de error hacia el emisor. Si la solicitud es aceptada, el ruteador enviará el RESV a lo largo de la ruta hacia el siguiente ruteador y los datos acerca del nivel requerido de QoS son pasados a los mecanismos del ruteador responsable del control de tráfico.
5. La recepción de la solicitud de reservación por el ruteador también significa que los parámetros de QoS se envían para procesamiento en unidades apropiadas del ruteador. El método específico del procesamiento del parámetro de QoS no se describe en RSVP. Sin

embargo, por lo regular consiste en que el ruteador verifique la disponibilidad del ancho de banda libre y la memoria requerida para la nueva reservación. Si esta verificación produce el resultado positivo, el ruteador almacenará los parámetros de reservación y los restos de los valores de contador correspondientes a los recursos apropiados.

6. Cuando el último ruteador a lo largo de la ruta hacia arriba recibe el mensaje RESV y acepta la solicitud, envía un mensaje de confirmación hacia el nodo de origen. Una vez realizada la reservación de grupo, los puntos de ramificación del árbol de entrega que tienen varios flujos reservados se unen y se tienen en cuenta. Por ejemplo, en el caso considerado, los mensajes RESV de los receptores C1 y C2 son unidos en el ruteador R1. Si se solicita el mismo ancho de banda para todos los flujos reservados, también se solicitará para el flujo reunido. Si se solicitan diferentes valores del ancho de banda, se elegirá el valor máximo para el flujo común.
7. Después de establecer un estado de reservación, el origen inicia la transmisión de los datos; a lo largo de toda la ruta hacia el receptor o receptores, los datos se sirven con la QoS especificada.

Es necesario destacar que el esquema descrito realiza la reservación solamente en una dirección. Para asegurar los parámetros requeridos de QoS de la transmisión de datos también en la dirección inversa dentro del marco de la sesión del usuario, se debe asegurar que el emisor y el receptor intercambien los papeles y lleven a cabo una vez más la reservación RSVP.

Para aplicar los parámetros de reservación al tráfico de datos, se debe asegurar que los mensajes RSVP y los paquetes de datos se trasladen a través de la red a lo largo de la misma ruta. Esto podrá asegurarse si los mensajes RSVP se transmiten con base en los mismos registros de la tabla de ruteo empleada para el tráfico del usuario.

NOTA *Si al transmitir los mensajes RSVP se utiliza el método tradicional de seleccionar los registros apropiados de la tabla de ruteo, se perderá la posibilidad de solucionar el valor completo de ingeniería de tráfico, pues todas las rutas posibles no se usarán para reservación. Por el contrario, solamente la ruta más corta seleccionada de acuerdo con alguna métrica de enrutamiento del protocolo de enrutamiento se empleará para este propósito.*

Puede cancelarse una reservación ya sea directa o indirectamente. La cancelación directa se lleva a cabo por el emisor o el receptor al utilizar mensajes apropiados de RSVP. La cancelación directa tiene lugar mediante tiempo límite: el estado de reservación tiene un TTL específico, igual que los registros dinámicos en las tablas de ruteo. De acuerdo con RSVP, el receptor debe confirmar periódicamente la reservación. Si los mensajes de confirmación dejan de llegar, se cancelará la reservación en cuanto expire su TTL. Una cancelación así se conoce como *cancelación suave* o *ligera*.

Se han diseñado muchas extensiones para RSVP, las cuales hacen este protocolo adecuado para más que la operación dentro de la arquitectura RSVP. Entre las soluciones más importantes están las extensiones de ingeniería de tráfico, utilizadas en MPLS y tecnologías generalizadas MPLS que se examinarán en la parte V.

20.3.5 Marco de servicios diferenciados

Los servicios DiffServ se basan en el mismo modelo de QoS generalizado que los servicios IntServ. Sin embargo, DiffServ considera las clases de tráfico como objetos de servicio en lugar de flujos individuales.

Recuérdese que la **clase de tráfico** es un conjunto de paquetes suministrados para procesamiento, que tienen los parámetros comunes; por ejemplo, éstos pueden ser todos los paquetes de aplicaciones de voz o todos los paquetes que tengan MTU y que se hallen dentro de los límites predefinidos.

En contraste con los flujos de datos, las clases de tráfico no se diferencian de los paquetes por sus rutas.

La figura 20.4 muestra esa diferencia. Así, el ruteador R1 relaciona todos los flujos que requieren servicio prioritario y que llegan en su interfase i1 a la misma clase de tráfico, sin importar qué ruta tan tardía pueda ser. El ruteador R2 funciona con otra clase de prioridad, pues no contaba con todos los flujos de la interfase i1 del ruteador R1.

Por lo regular la red DiffServ soporta servicios diferenciados o un pequeño número de clases de tráfico, por ejemplo, dos (el tráfico sensible al retardo y el elástico) o tres (cuando además del tráfico sensible al retardo y el elástico se soporta otra clase de tráfico, que requiere entrega garantizada de los paquetes con el mínimo predefinido de la velocidad del tráfico). El número pequeño de clases de tráfico asegura la escalabilidad de este modelo, pues los ruteadores no necesitan almacenar los estados de cada flujo individual del usuario. Además, la alta escalabilidad de DiffServ se asegura gracias a que todo ruteador toma su decisión acerca del servicio proporcionado a un flujo agregado específico. Esta decisión se toma de forma independiente y no necesita estar coordinada con otros ruteadores. Un enfoque así se conoce como *comportamiento por hop* (*PHB,* por las siglas para *Per Hop Behavior*).

De conformidad con lo anterior, como la arquitectura DiffServ no rastrea rutas de paquete, no se utiliza el protocolo de señalización de reservación de recursos, semejante a RSVP en

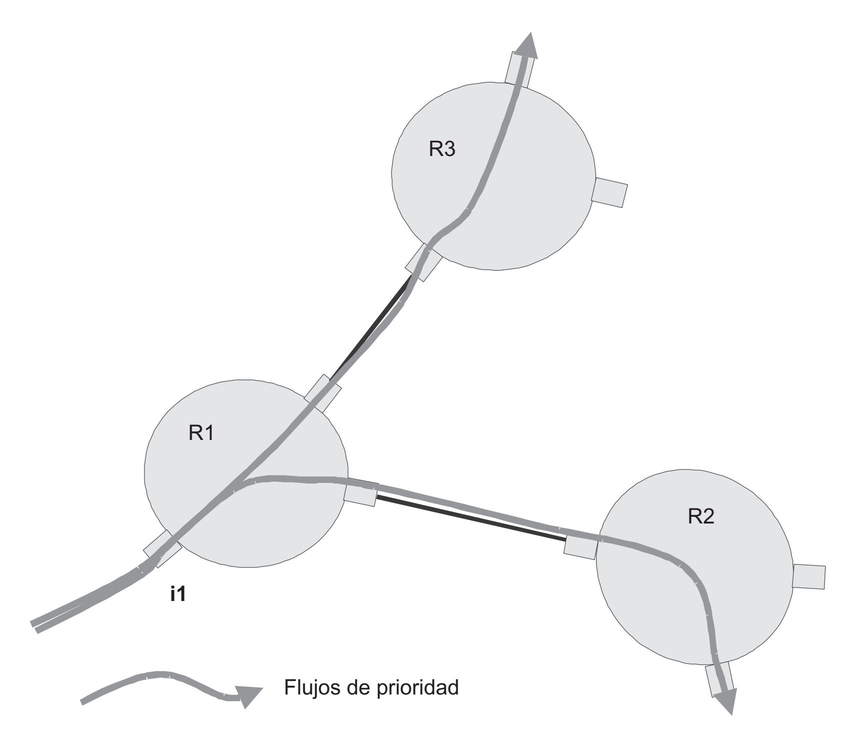


FIGURA 20.4 En contraste con IntServ, DiffServ considera los flujos agregados como objetos de servicio en lugar de flujos individuales.

la arquitectura IntServ. En su lugar, los ruteadores de red realizan reservación de recursos estática para cada una de las clases de tráfico soportadas por la red.

En DiffServ, una etiqueta conducida por el campo *IP Precedente* o por su sucesor, el campo *DiffServ byte*, se utiliza como un atributo y especifica que el paquete IP pertenece a cierta clase de tráfico.

Como se muestra en la figura 20.5, aunque el campo *DS* usa el campo *TOS*, redefine los valores del IP de este campo como definidos anteriormente en los RFCs apropiados (791, 1 122 y 1 349). En la actualidad sólo se utilizan los seis bits más significativos del campo *DS-byte* y únicamente se emplean los tres bits más significativos para definir la clase de tráfico (lo que proporciona la posibilidad de tener normas de ocho clases diferentes). El bits menos significativo (fuera de los seis bits empleados) del campo *DS-byte* suele conducir el atributo *IN* e indica que el paquete se ha "abandonado" del perfil del tráfico (semejante a los atributos *DE* de la tecnología *frame relay* o el *CPL* de la tecnología ATM). Los dos bits intermedios describen diversas variantes de servicio del paquete dentro de la misma clase de tráfico.

El ruteador que soporta DiffServ debe soportar los procesos de clasificación, marcado, medición y acondicionamiento del tráfico, además de su uniformidad y servicio en la cola de prioridad o de prioridad ponderada.

Aunque cada ruteador de red puede marcar paquetes, el modelo DiffServ considera que el marcado de paquetes en el punto de entrada de la red es la variante principal. Este punto de entrada a la red debe soportar el protocolo DiffServ y estar bajo control administrativo de una sola organización. Una red así se conoce como *dominio DiffServ*. A medida que los paquetes abandonan el dominio DiffServ, se elimina el marcado de modo que otro dominio pueda volver a aplicarlo. Los ruteadores fronterizos de DiffServ desempeñan el papel de los puntos de verificación del dominio. Verifican el tráfico entrante y determinan si tiene derecho a los servicios diferenciados.

El protocolo DiffServ supone la existencia de un acuerdo de licencia de servicio (SLA, Service License Agreement) entre dominios que tienen una frontera común. A su vez, el SLA especifica criterios de política y define el perfil del tráfico. Se espera que el tráfico se forme en los puntos de salida del dominio de acuerdo con el SLA y que en el punto de entrada del dominio el tráfico se determinará de acuerdo con las reglas de la política. Cualquier tráfico que se encuentre fuera del perfil (por ejemplo, el tráfico que exceda los límites superiores del ancho de banda especificado en el SLA) no tendrá garantías de servicio (o simplemente pagará por las velocidades altas de acuerdo con el SLA). Los criterios de la política pueden

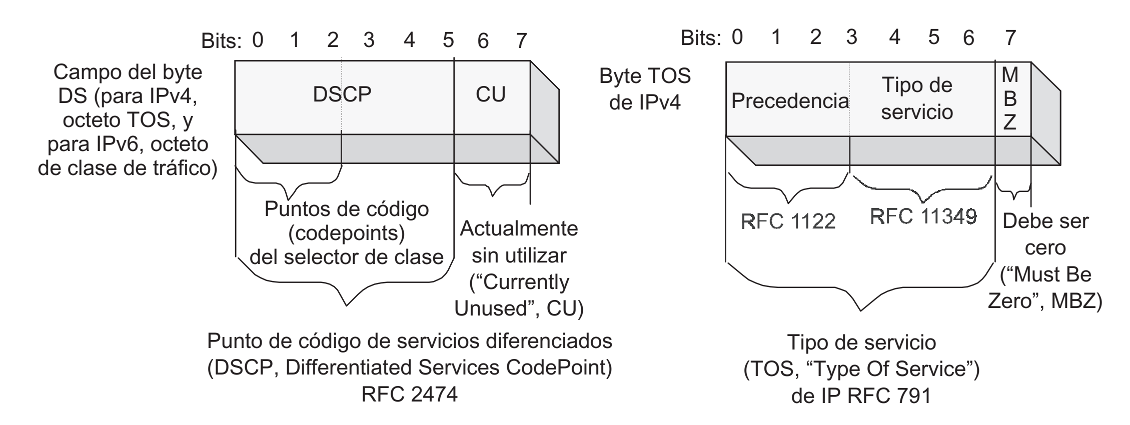


FIGURA 20.5 Correspondencia de los campos del byte DS con los campos de los bytes TOS.

incluir la hora del día, las direcciones de origen y destino, el protocolo de transporte y los números de puerto. Cuando se observan las reglas de la política y el tráfico satisface el perfil predefinido, el dominio DiffServ debe asegurar el servicio de este tráfico con los parámetros de QoS definidos en SLA.

Por el momento, IETF ha desarrollado dos estándares para el envío de paquetes paso a paso (PHB), lo cual representa dos servicios diferentes:

- *Direccionamiento expedito (EF, Expedited Forwarding).* Este tipo de servicio se caracteriza por un solo valor de código (10111) y proporciona el nivel más alto de QoS, minimizando los retardos y las variaciones de retardo. Cualquier tráfico cuya intensidad exceda la intensidad especificada por el perfil del tráfico es descartado.
- *Direccionamiento asegurado (AF, Assured Forwarding).* En este tipo de servicio existen cuatro clases de tráfico y tres niveles de descarte de paquetes en cada clase, lo que agrega hasta 12 tipos de tráfico. Cada clase de tráfico está asignada a un ancho de banda mínimo predefinido y tamaño de búfer para almacenar su cola. El tráfico que excede el perfil es entregado con un nivel de probabilidad inferior al de tráfico que satisface la condición del perfil. Esto significa que se puede otorgar el servicio al tráfico que está fuera del perfil con calidad inferior, pero no necesariamente se descartará.

Con base en esas especificaciones paso a paso y SLA apropiados, es posible dar a los usuarios finales servicios de extremo a extremo: servicios EF y servicios AF, respectivamente.

El objetivo principal del servicio EF es proporcionar la QoS comparable con la de las líneas dedicadas. Debido a ello, este servicio también se conoce como *servicio de línea virtual dedicado* o como servicio Premium (Premium Service), que destaca la QoS más alta en redes IP DiffServ. Posteriormente, esta especificación se hizo obsoleta mediante RFC 3246, que da una definición más precisa del servicio EF.

Si el servicio EF se pone en marcha mediante el mecanismo que permite el descarte ilimitado de otro tráfico (por ejemplo, una cola de prioridad), su implementación deberá incluir algunas herramientas para limitar la influencia del tráfico EF sobre otras clases de tráfico. Por ejemplo, esto puede hacerse al establecer la limitación sobre la velocidad del tráfico EF en la entrada del ruteador al utilizar el algoritmo de cubeta de estafetas. La velocidad máxima del tráfico EF y posiblemente el tamaño de ráfaga debe establecerlos el administrador de la red.

Cuatro grupos de servicios AF están orientados hacia la entrega garantizada, pero sin la minimización del nivel de retardo de paquetes, como se estipula para el servicio EF. La entrega está garantizada únicamente cuando la velocidad del tráfico entrante no excede la entrega de ancho de banda mínimo asignada para esta clase. La implementación de los servicios AH está bien combinada con el servicio EF, pues puede emplearse el tráfico EF de acuerdo con el método de prioridad, pero con intensidad ilimitada del flujo de entrada. El ancho de banda restante se distribuye entre las clases de tráfico del servicio AF según el algoritmo de procesamiento de cola ponderada. Esto asegurará el ancho de banda requerido. No obstante, no se minimizarán los retardos. La implementación del servicio AF sugiere (pero no requiere) usar tanto el procesamiento de la cola ponderada para cada clase con ancho de banda reservado, como la retroalimentación RED.

La relativa simplicidad del servicio de tráfico al utilizar DiffServ determina sus inconvenientes. La principal desventaja es la dificultad de proporcionar garantías cualitativas a los suscriptores de servicio. Considérese esta desventaja en el ejemplo de la red mostrada en la figura 20.6.

Las clases de tráfico que dan servicio suponen que los ruteadores fronterizos vigilan el tráfico sin tener en cuenta las direcciones de destino del paquete. Este enfoque puede llamarse

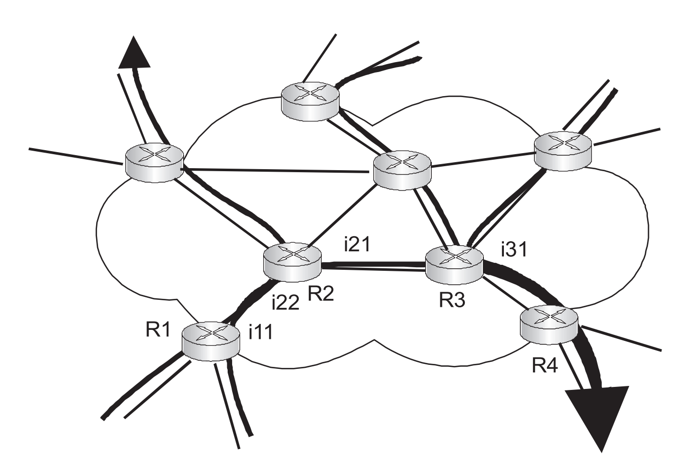


FIGURA 20.6 Incertidumbre de los servicios DiffServ.

destino inconsciente. Por lo regular, para las interfases de entrada de los ruteadores fronterizos se especifica algún límite predefinido de la carga de trabajo permitida para cada clase de tráfico. Por ejemplo, supóngase que la red da servicio al tráfico de dos clases: *Premium* y *Best Effort (Mejor Esfuerzo)*. El umbral para el tráfico Premium se establece al 20% para toda interfase de entrada de cada ruteador fronterizo. Aparte de esto, supóngase, por simplicidad, que todas las interfases de todos los ruteadores de la red tienen el mismo ancho de banda.

Evidentemente, a pesar de esta limitación algo estricta, las interfases de los ruteadores de red tendrán cargas diferentes. Por simplicidad, la figura 20.6 muestra sólo los flujos que requieren el servicio Premium. De este modo, la interfase de salida i11 del ruteador R1 da servicio a dos flujos de servicio Premium y tiene una carga de 40%, mientras que la interfase de salida i21 del ruteador R2 sirve solamente a un flujo así, pues el segundo flujo va a través de otra interfase de salida. En cuanto a la interfase de salida i31 del ruteador R3, está sobrecargado, porque sirve a tres flujos de servicio Premium; en consecuencia, su coeficiente de utilización es de 60%. Con base en los factores que influyen en la generación de la cola (véase el *capítulo 7*), usted sabe que el coeficiente de utilización es el factor más significativo y sus valores críticos están alrededor de 50%. Por lo tanto, las colas largas de los paquetes de servicio Premium se generarán en la interfase i31. Estas colas rebajarán la QoS, porque producen considerables retardos e incluso conducen a pérdidas de paquetes. El tráfico de la clase del Mejor Esfuerzo también será afectado, pues tiene sólo 40% del ancho de banda de la interfase.

Naturalmente, hemos simplificado el patrón, pues las interfases de los ruteadores troncales suelen ser más rápidas que las correspondientes a los ruteadores fronterizos; por lo tanto, sus coeficientes de utilización serán menores que la suma de los coeficientes de utilización de las interfaces de entrada, como en este ejemplo. Para reducir la probabilidad de sobrecargar las interfaces internas de los ruteadores troncales y las interfases de salida de los ruteadores fronterizos, también es posible disminuir el umbral permitido para la carga de tráfico Premium en la interfase de entrada, por ejemplo, a 5 por ciento.

A pesar de ello, todas esas medidas no garantizan que las interfases de los ruteadores de la red funcionen en el intervalo requerido del coeficiente de utilización y, en consecuencia, aseguren la QoS requerida. Para suministrar tales garantías, es necesario utilizar métodos de ingeniería de tráfico, por ejemplo, para controlar flujos de tráfico en lugar de clases o, en este caso, flujos agregados. Un **flujo agregado** es el flujo que abarca paquetes de la misma

clase y tiene una parte común de la ruta a través de la red. Esta parte común no necesita incluir la trayectoria completa desde la interfase de entrada de un ruteador fronterizo hasta la interfase de salida de otro ruteador fronterizo. Para los paquetes, es suficiente pasar al menos dos interfases en común para considerar que es un flujo agregado. Por ejemplo, éste es el caso con las interfases de paso del flujo i11 e i22 en la figura 20.6.

Entonces, al conocer la ruta a lo largo de la cual pasa cada flujo agregado a través de la red, es posible verificar si existen suficientes recursos a lo largo de la ruta para cada flujo. Por ejemplo, se debe verificar si los coeficientes de utilización de la interfase exceden el valor de umbral predefinido. Para conseguir esto, es necesario utilizar vigilancia con la cuenta de la dirección de destino de los paquetes, por ejemplo, usar *vigilancia consciente del destino*. Sin embargo, la puesta en práctica de un enfoque así en redes IP encuentra varias dificultades. En primer lugar, la tecnología DiffServ no emplea el protocolo de señalización como RSVP o la tecnología IntServ. Esto significa que todas las verificaciones de la disponibilidad de recursos en los ruteadores para cada flujo agregado deben llevarse a cabo en el modo fuera de línea, manualmente o al usar algún software especial. En segundo lugar, para realizar tales cálculos, se deben conocer las trayectorias de los flujos a través de la red. Tales rutas están determinadas por las tablas de ruteo construidas al utilizar algún protocolo de enrutamiento, como RIP u OSPF; al usar una combinación, si diversos protocolos de enrutamiento de la clase IGP se emplean en la red, o manualmente. Por ende, para cálculos manuales o automatizados, es necesario conocer las tablas de ruteo de todos los ruteadores de la red y rastrear sus cambios. Ésta no es una tarea trivial, si se tiene en cuenta que las fallas de los enlaces de red o ruteadores reconstruyen tales tablas. Además, se debe considerar que los ruteadores pueden aplicar métodos de equilibrio de carga, dividiendo el flujo agregado en diversos flujos, lo cual también hace más complicados los cálculos.

Una versión de DiffServ consciente del destino incrementa la QoS proporcionada por el portador de comunicaciones. Sin embargo, también complica la idea del método, que está basado en el servicio independiente de clases de tráfico por cada ruteador de la red.

20.4 TRADUCCIÓN DE DIRECCIÓN DE RED

PALABRAS CLAVE: seguridad, escasez de direcciones, traducción de dirección de red (NAT, Network Address Translation), direcciones privadas, NAT tradicional, dispositivo NAT, dirección de red y traducción de puerto (NAPT, Network Address and Port Translation), anuncios de ruteo, y sesiones entrantes y salientes.

El ruteo en Internet se lleva a cabo con base en las direcciones de destino colocadas en los encabezados del paquete. Como regla, estas direcciones permanecen sin cambios desde que las forma el emisor y hasta que llegan al nodo de destino. Sin embargo, esta regla tiene algunas excepciones. Por ejemplo, en la ampliamente utilizada tecnología de **traducción de las direcciones de la red** (**NAT**), se supone que el paquete es enviado a la Internet externa a partir de las direcciones utilizadas para enrutamiento del paquete en la red interna de la compañía.

20.4.1 Razones para la traducción de dirección

Una de las razones más conocidas para utilizar la tecnología NAT es la escasez de direcciones IP. Si por alguna razón una compañía que necesita conectarse a Internet no puede recibir el número requerido de direcciones IP globales del proveedor, puede emplear la tecnología

NAT. En este caso, se usan **direcciones reservadas (privadas)** para direccionar los hosts internos, descritos en el *capítulo 17*.

Para habilitar los hosts con direcciones privadas con el fin de comunicarse utilizando Internet o para conectar a los hosts que tienen direcciones globales, es necesario emplear la tecnología NAT.

La tecnología NAT prueba su utilidad cuando una compañía necesita ocultar las direcciones de los hosts dentro de sus redes internas por consideraciones de seguridad. Esto evita que los intrusos aprendan la estructura y escala de la red, además de la intensidad del tráfico entrante y saliente.

20.4.2 NAT tradicional

La tecnología NAT tiene diversas variantes, entre las cuales la más conocida es la **NAT tradicional**, que permite que los hosts de la red privada tengan acceso a los hosts localizados en redes externas de una forma transparente para los usuarios. Cabe destacar que esta variante de NAT resuelve el problema de organización sólo en sesiones de conexión **salientes**. La dirección de la sesión en este caso se halla determinada por la ubicación de su iniciador. Si el intercambio de datos se inicia con la aplicación realizada en algún host localizado en la red interna, esta sesión se denominará *saliente* aunque los datos del exterior se entreguen dentro de la red interna durante esta sesión.[2]

La idea de NAT está basada en el enfoque siguiente (figura 20.7): supóngase que una red corporativa forma un dominio pequeño, cuyos hosts tienen asignadas direcciones privadas. El software NAT se halla instalado en el ruteador de conectar la red de la compañía con la red externa. NAT mapea dinámicamente el conjunto de direcciones privadas IP {IP*} al conjunto de direcciones IP globales {IP}, obtenidas por la compañía desde el ISP y asignadas a la interfase externa del ruteador de la compañía.

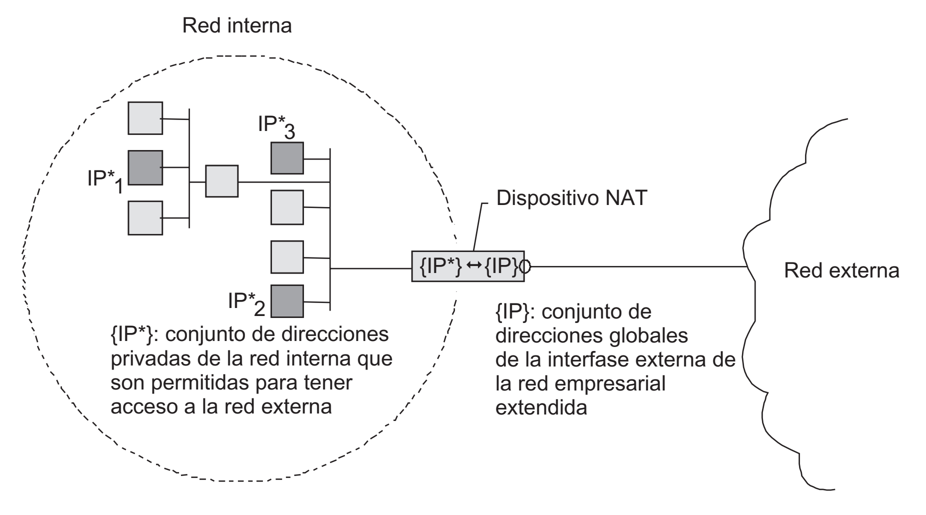


FIGURA 20.7 Método de NAT tradicional.

[2] El NAT tradicional permite sesiones en dirección inversa solamente como una excepción. Para este propósito, utiliza mapeo de dirección estática destinado a algún conjunto limitado de hosts para el cual se especifica un mapeo único y no ambiguo entre las direcciones internas y externas.

Una propiedad importante de la operación de NAT es la regla de acuerdo con la cual los anuncios de la ruta se propagan a través de las fronteras de las redes privadas. Los anuncios de protocolos de enrutamiento acerca de las redes externas son pasados por los ruteadores fronterizos hacia las redes internas y los procesan los ruteadores internos. Sin embargo, la afirmación inversa no es verdadera. Los ruteadores de redes externas no reciben anuncios acerca de redes internas, pues tales anuncios son filtrados cuando pasan información hacia interfases externas. Por lo tanto, los ruteadores internos "conocen" las rutas hacia todas las redes externas, mientras que los ruteadores externos no tienen información acerca de la existencia de las redes privadas.

La NAT tradicional se subdivide en **traducción básica de las direcciones de la red** (NAT básica), el método que utiliza solamente direcciones IP para el mapeo, y **traducción del puerto de las direcciones de la red** (NAPT, Network Address Port Translation), el método para mapear direcciones e identificadores de transporte que se usan. Con mucha frecuencia, los puertos TCP/UDP se utilizan como identificadores de transporte.

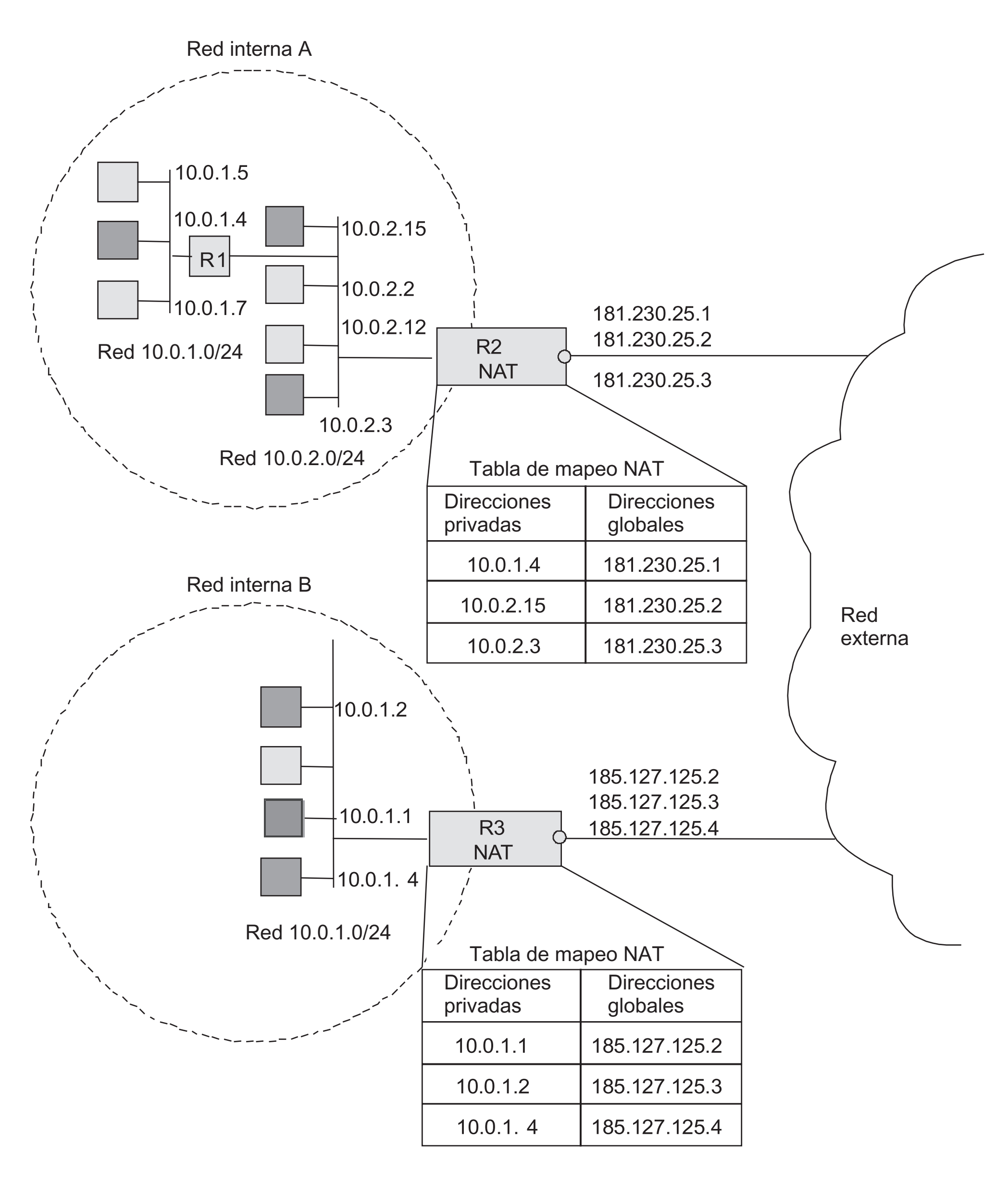
20.4.3 NAT básica

Si el número de hosts locales para el que es necesario asegurar el acceso a la red externa no excede la cantidad de direcciones globales disponibles, se podrá garantizar el mapeo único entre direcciones privadas y globales. En cualquier momento, el número de hosts internos que tienen la posibilidad de interactuar con la red externa está limitado por la cantidad de direcciones globales disponibles. En esta situación, el uso de NAT es dirigido principalmente para garantizar la seguridad, más que para resolver el problema de la escasez de direcciones.

Las direcciones privadas de algunos hosts pueden mapearse *estáticamente* a direcciones globales. Asimismo, se podrá tener acceso a tales hosts desde el exterior si se utiliza la dirección global asignada a ellos. El mapeo de las direcciones internas y externas está especificado por la tabla soportada por el ruteador de red o cualquier otro dispositivo (por ejemplo, un muro de fuego) en el que se encuentra instalado el software NAT.

Los dominios de extremo terminal pueden utilizar direcciones privadas coincidentes. Por ejemplo, las redes A y B (figura 20.8) usan el mismo bloque de direcciones para direccionamiento interno: 10.0.1.0/24. Al mismo tiempo, las direcciones de interfases externas de ambas redes (181.230.25.1/24, 181.230.25.2/24 y 181.230.25.3/24 en la red A y 185.127.125.2/24, 185.127.125.3/24 y 185.127.125.4/24 en la red B) son globalmente únicas. Ningún otro host en la interred las emplea. En este ejemplo, solamente tres hosts en cada una de las redes puede ir "fuera" de los límites de la red a la compañía. La correspondencia estática de las direcciones privadas de estos hosts para las direcciones globales se especifica en la tabla de ruteo de los dispositivos fronterizos de ambas redes.

Cuando el host 10.0.1.4 de la red A envía un paquete al host 30.0.1.2 de la red B, coloca la dirección global 185.127.125.3/24 en el campo de dirección de destino del encabezado del paquete. El nodo de origen envía un paquete a su ruteador predeterminado, R1, el cual conoce la ruta hacia la red 185.127.125.0/24. El ruteador pasa el paquete al ruteador fronterizo R2, que también conoce la ruta hacia la red 185.127.125.0/24. Antes de enviar un paquete, el protocolo NAT que se ejecuta en este ruteador fronterizo utiliza la tabla de mapeo para reemplazar la dirección privada 10.0.1.4 especificada en el campo de dirección de origen con su dirección global correspondiente: 181.230.25.1/24. Cuando el paquete llega a la interfase externa del dispositivo NAT de la red B después de viajar a través de la interred, la dirección de destino global 185.127.125.3/24 se transforma en la dirección privada 10.0.1.2. Los paquetes enviados en la dirección inversa experimentan el mismo procedimiento de traducción de dirección.



Direcciones privadas	Direcciones globales
10.0.1.4	181.230.25.1
10.0.2.15	181.230.25.2
10.0.2.3	181.230.25.3

Direcciones privadas	Direcciones globales
10.0.1.1	185.127.125.2
10.0.1.2	185.127.125.3
10.0.1. 4	185.127.125.4

FIGURA 20.8 NAT básica: traducción de dirección para sesiones salientes.

Nótese que en la operación anteriormente descrita no se requiere que participen los nodos emisor y receptor, lo cual significa que este procedimiento es transparente para los usuarios.

20.4.4 Traducción de puerto y dirección

Supóngase que alguna organización tiene una red IP privada conectada a la red del ISP mediante un enlace WAN. La interfase externa del ruteador fronterizo R2 tiene asignada una dirección global y todos los otros hosts de la red empresarial tienen asignadas direcciones privadas. NAPT permite que *todos* los hosts de la red interna se comuniquen simultáneamente con redes externas mediante el uso de una sola dirección IP registrada. Cabe plantear una pregunta obvia: ¿cómo pueden encontrar el host emisor los paquetes externos que llegan *en*

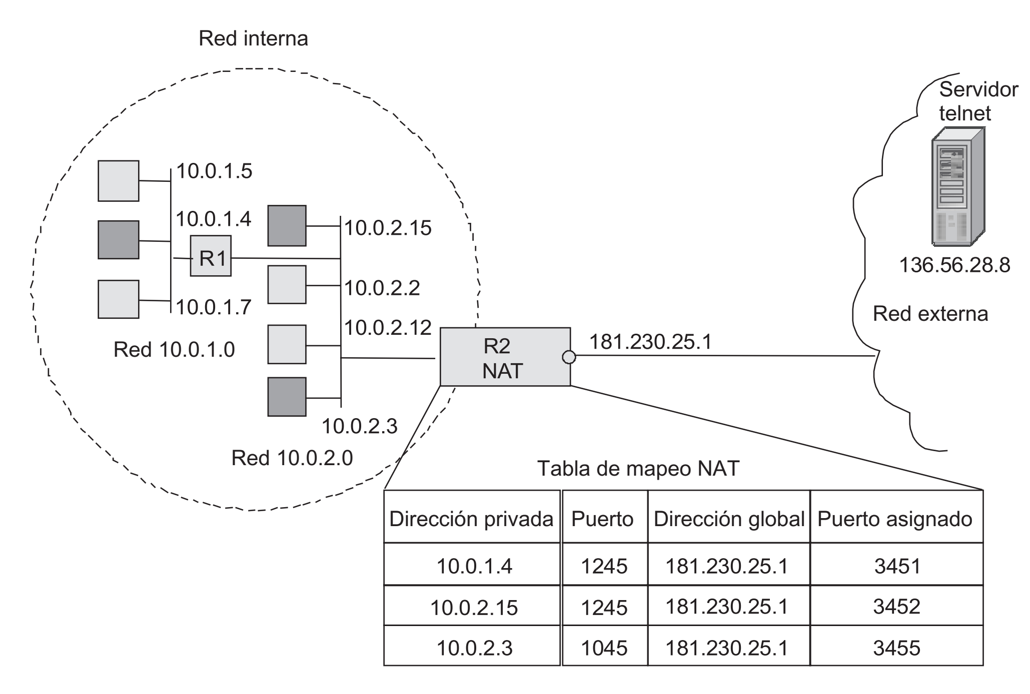
respuesta a las solicitudes provenientes desde esta red privada? Después de todo, los campos de dirección de origen de los paquetes enviados hacia la red externa contienen la misma dirección: la dirección de la interfase externa del ruteador fronterizo.

Para la identificación única del host emisor se utiliza información adicional. Si un paquete IP encapsula los datos de UDP o TCP, se usarán números de puerto UDP o TCP como esa información adicional. Sin embargo, esto no aclara completamente el asunto, pues pueden originarse varias solicitudes desde la red interna que tengan números de puerto de emisor coincidentes. En consecuencia, surge otra vez la cuestión acerca de asegurar la conciencia única y sin ambigüedad de una sola dirección global para el conjunto de direcciones privadas internas. La solución depende de que, cuando el paquete pasa desde la red interna a la externa, cada par *{dirección privada interna; número de puerto TCP/UDP del emisor}* es mapeado al par *{dirección IP global de la interfase externa; número de puerto TCP/UDP asignado}*. El número de puerto asignado se elige arbitrariamente, pero debe ser único entre todos los hosts que tienen acceso a la red externa. Este mapeo se registra en la tabla.

Dicho modelo satisface los requerimientos de la mayoría de las redes de tamaño medio para tener acceso a redes externas al utilizar una sola dirección IP registrada que se ha obtenido de un proveedor.

La figura 20.9 muestra un ejemplo en el que la red A de extremo terminal usa direcciones internas desde el bloque de dirección 10.0.0.0. La interfase externa del ruteador de esta red tiene la dirección 181.230.25.1, asignada por el ISP.

Cuando el host 10.0.1.4 de la red interna envía un paquete al servidor de telnet localizado en la red externa, emplea su dirección global 136.56.28.8 como la dirección de destino. El paquete llega al ruteador R1, que sabe que la ruta a la red 136.56.0.0/16 va a través del ruteador fronterizo R2. La NAPT del ruteador R2 traduce la dirección 10.0.1.4 y el puerto TCP 1245 de origen a la dirección globalmente única 181.230.25.1 y el puerto TCP unívocamente asignado (3451, en este ejemplo). De esta forma, el paquete es enviado hacia la red externa y



Dirección privada	Puerto	Dirección global	Puerto asignado
10.0.1.4	1245	181.230.25.1	3451
10.0.2.15	1245	181.230.25.1	3452
10.0.2.3	1045	181.230.25.1	3455

FIGURA 20.9 NAPT: traducción de dirección y número de puerto para sesiones salientes TCP/UDP.

alcanza el servidor de telnet. Cuando el receptor genera un mensaje de respuesta, especifica solamente la dirección global registrada de la red interna como la dirección de destino. Ésta es la dirección de la interfase externa del dispositivo NAPT. Como el número de puerto del receptor, el servidor especifica el número de puerto TCP asignado tomado desde el campo del número de puerto del emisor del paquete que ha recibido. Cuando el paquete de réplica llega al dispositivo NAPT de la red interna, el número de puerto se utiliza para seleccionar la línea requerida de la tabla de traducción. Mediante esa línea, se definen la dirección IP interna del host apropiado y su número de puerto real. Este procedimiento de traducción es por completo transparente para nodos terminales.

NOTA *Adviértase que la tabla de traducción contiene otro registro con número de puerto 1245. Esta situación es posible, pues los sistemas operativos que se ejecutan en computadoras distintas asignan números de puerto a programas cliente de manera independiente. Es esta ambigüedad para la eliminación de la cual se utiliza el número de puerto asignado único.*

La variante NAPT permite que partan solamente sesiones TCP/UDP desde la red privada. Sin embargo, puede ser necesario asegurar el acceso a algún modo de la red interna desde el exterior. En el caso más simple, cuando el servicio es el registrado (o sea, el servicio tiene asignado un número de puerto bien conocido, por ejemplo, web o DNS) y este servicio está representado dentro de una red interna en una instancia simple, este problema se resuelve de manera relativamente fácil. El servicio y el host en el cual funciona se definen unívocamente por medio de un número de puerto bien conocido registrado de ese servicio.

Para concluir la consideración de la tecnología NAT, obsérvese que aparte de la NAT tradicional existen otras variantes de NAT. Un ejemplo de una variante así es la NAT doble, cuando las direcciones de origen y destino son modificadas, en contraste con la NAT tradicional, cuando solamente una dirección es modificada. La NAT doble es necesaria cuando los espacios de dirección privada y externa tienen colisiones. Con más frecuencia, esto ocurre cuando un dominio interno tiene asignadas de manera incorrecta direcciones públicas que pertenecen a otra organización. Esta situación también podría surgir si la red de una organización hubiese sido aislada inicialmente del monto exterior y las direcciones (tomadas desde un espacio de dirección global) hubieran sido asignadas de forma arbitraria. En ocasiones puede surgir una colisión debido al cambio del ISP cuando la organización quiere mantener las direcciones antiguas para los hosts de la red interna.

20.5 RUTEADORES

PALABRAS CLAVE: ruteador, tabla de ruteo, interfase del ruteador, acceso a los medios, señales de bit de formación, recepción de trama, cálculo de CRC, ARP, ruteadores troncales, ruteadores de borde u orilla, ruteadores de portadora, ruteadores de software, organización de multiprocesador de ruteadores de oficina remota y LAN y SO de ruteador.

20.5.1 Funciones del ruteador

La función principal del ruteador es leer los encabezados de los paquetes de red recibidos y almacenados temporalmente en un búfer en cada puerto (por ejemplo, IPX, IP, AppleTalk o DECnet). Después de eso, con base en la dirección de red del paquete, el ruteador decide su ruta. Como regla, esta dirección incluye el número de red y el número de host.

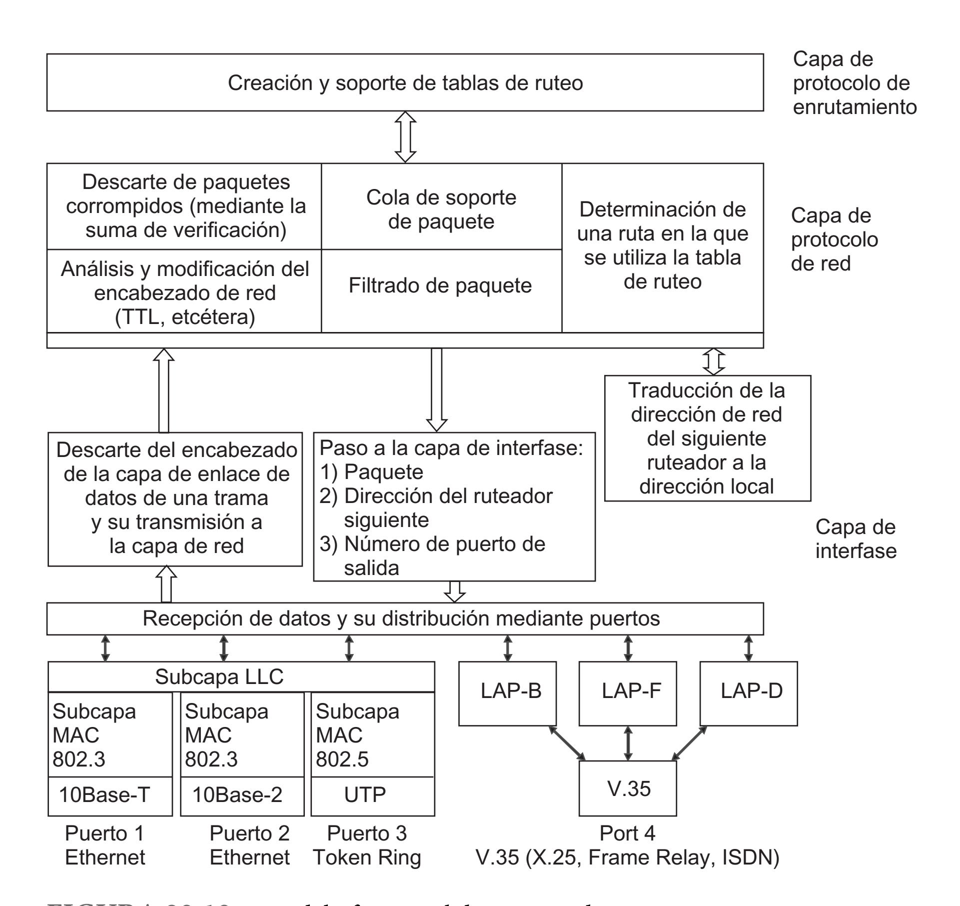


FIGURA 20.10 Modelo funcional de un ruteador.

Las funciones del ruteador pueden dividirse en tres grupos de acuerdo con las capas del modelo OSI (figura 20.10).

Nivel de interfase

En la capa inferior, el ruteador, como cualquier dispositivo conectado a la red, asegura la interfase física para el medio de transmisión, incluidos la coordinación de los niveles de señal eléctrica, la codificación lógica y de línea y el equipamiento del ruteador con un tipo específico de conector. En diferentes modelos de ruteadores, diversos conjuntos de interfaces físicas suelen proporcionarse como combinaciones de puertos para conectar LAN y WAN. El protocolo de capa de enlace de datos específico está vinculado inseparablemente con cada interfase, por ejemplo: Ethernet, Token Ring o FDDI. Las interfases para conexión a las WAN determinan a menudo sólo algún estándar de capa física. Sobre este estándar, pueden funcionar varios protocolos de capa de enlace de datos dentro de un ruteador. Por ejemplo, un puerto WAN puede soportar la interfase V.35 sobre la cual varios protocolos de capa de enlace de datos pueden funcionar: PPP (transmite el tráfico de IP y otros protocolos de capa de red), LAP-B (utilizado en redes X.25), LAP-F (usado en red de retardo de trama), LAP-D (empleado en redes ISDN) y ATM. La diferencia entre interfases LAN y WAN se explica mediante las tecnologías LAN, que determinan los estándares tanto de la capa de enlace de datos como física que pueden utilizarse sólo en combinación.

Las interfases del ruteador realizan un conjunto completo de funciones de capa de enlace de datos y física relacionadas con la transmisión de la trama, incluidos el acceso a los medios (si es necesario), las señales de bit de formación, la recepción de tramas, el cálculo de sumas de verificación y el paso del campo de datos de la trama al protocolo de capa superior si la suma verificadora tiene el valor correcto.

NOTA *Como cualquier nodo terminal normal, cada puerto del ruteador tiene sus direcciones de hardware (en las LANs, ésta es una dirección MAC) mediante la cual los otros nodos envían tramas que requieren enrutamiento.*

La lista de interfases de capa física soportada por un modelo de ruteador especificado es la característica más importante para el consumidor. El ruteador debe soportar todos los protocolos de capa física y de enlace de datos utilizados en cada una de las redes a las cuales se conectará directamente. La figura 20.10 muestra el modelo funcional de un ruteador que tiene cuatro puertos que incrementan las siguientes interfases físicas: 10Base-T y 10Base-2 para dos puertos Ethernet, UTP para Token Ring y V.35 sobre el cual los protocolos LAP-B, LAP-D o LAP-F pueden funcionar, lo que asegura la posibilidad de conexión para X.25, ISDN, o redes Frame Relay.

Las tramas suministradas a dos puertos del ruteador, después del procesamiento mediante los protocolos apropiados de capa de enlace de datos y física, se desmontan desde los encabezados de la capa de enlace de datos. Los datos recuperados desde el campo de datos de la trama se pasan a la entidad del protocolo de capa de red.

Protocolo de capa de red

El protocolo de red, a su vez, recupera desde el paquete el encabezado de capa de red y **analiza y corrige el contenido de sus campos**. En primer lugar, es necesario probar la suma verificadora; si el paquete está corrompido, debe descartarse. Posteriormente una verificación determina si el tiempo que el paquete ha pasado en la red excede el umbral permitido (conocido como TTL). Si este tiempo excede el TTL, también se descartará el paquete. En esta etapa, todas las correcciones requeridas se incluyen en el contenido de algunos campos, por ejemplo: si es necesario, el TTL del paquete se incrementa o se vuelve a calcular su suma de verificación.

La función más importante del ruteador, el **filtrado**, también se llevará a cabo mediante la capa de red del ruteador. El paquete de capa de red encapsulado en el campo de datos de la trama para puentes o ruteadores está representado como una secuencia binaria no estructurada. Por otra parte, el software del ruteador contiene la entidad del protocolo de capa de datos y, en consecuencia, es capaz de analizar sintáctica o gramaticalmente las tramas y **analizar los campos individuales**. Este software se halla equipado con herramientas de GUI avanzadas que permiten a los administradores especificar reglas sofisticadas de filtrado sin problemas serios. Como regla, los ruteadores también pueden analizar la estructura de los mensajes de la capa de transporte. En consecuencia, los filtros pueden evitar que pasen dentro de la red mensajes de ciertos servicios de aplicación, como el servicio de telnet. Esta clase de filtrado se realiza al analizar el campo del tipo de protocolo en el mensaje de transporte.

La función principal de ruteo del ruteador, la determinación de las rutas, también se relaciona con la capa de red. La entidad del protocolo de capa de red utiliza el número de red recuperado del encabezado del paquete para encontrar la línea de la tabla de ruteo que contiene la dirección de red del siguiente ruteador y el número de puerto al cual es necesario pasar este paquete para asegurar que viaja en la dirección correcta.

Antes de que la dirección de red del siguiente ruteador se pase a la capa de enlace de datos, debe convertirse a la dirección local de acuerdo con la tecnología de red utilizada en la red que contiene el siguiente ruteador. Para este propósito, el protocolo de red solicita el *protocolo de resolución de dirección* (ARP).

Desde la capa de red, la dirección local del siguiente ruteador y el número de puerto del ruteador se pasan a la capa de enlace de datos. Con base en el número de puerto especificado, el paquete se conmuta a una de las interfases del ruteador, donde el paquete se encapsula en la trama del formato apropiado. La dirección local del siguiente ruteador se coloca en el campo de dirección de destino del encabezado de la trama. Después de eso, la trama se envía hacia la red.

Capa de protocolos de enrutamiento

Los protocolos de red utilizan activamente la tabla de ruteo en el curso de su operación. A pesar de ello, no se involucran en su operación o en el mantenimiento de su contenido. Estas funciones se delegan a los protocolos de enrutamiento. Con base en estos protocolos, los ruteadores intercambian información acerca de la topología de la red y luego analizan los datos recibidos para determinar las mejores rutas de acuerdo con criterios específicos. Los resultados de este análisis conforman el contenido de las tablas de ruteo.

Aparte de las funciones enumeradas, pueden delegarse otras funciones a los ruteadores, por ejemplo, las operaciones relacionadas con la fragmentación.

20.5.2 Clasificación de los ruteadores por áreas de aplicación

Por sus áreas de aplicación, los ruteadores se dividen en varias clases (figura 20.11).

Los *ruteadores troncales* están destinados a construir la red central de un portador de comunicaciones o corporación grande. Los ruteadores troncales funcionan sobre flujos de información agregada que conducen los datos de muchas conexiones del usuario.

La principal intención del ruteador troncal consiste en crear un núcleo de conmutación confiable y de alto rendimiento de la red. Para llevar a cabo esta tarea, los ruteadores troncales están equipados con interfases de alto rendimiento, como ATM de 155/622 Mbps, Gigabit Ethernet y 10 Gigabit Ethernet, además de interfases SONET/SDH que aseguran velocidades desde 155 Mbps hasta 10 Gbps. Para crear una topología de núcleo tolerante a fallas, los ruteadores troncales deben soportar varias de estas interfases.

Naturalmente, para evitar cuellos de botella en el núcleo de la red, el ruteador troncal debe proporcionar un rendimiento muy alto. Por ejemplo, si el ruteador está equipado con ocho interfaces de 10 Gbps (Ethernet o SDH), su rendimiento total deberá ser de 80 Gbps. Para conseguir tal rendimiento, los ruteadores troncales tienen una arquitectura interna distribuida semejante a la arquitectura de los conmutadores LAN, la cual se examinó en el *capítulo 15*. Cada puerto o grupo de puertos está equipado con su procesador que envía paquetes IP por cuenta propia, con base en la copia local de la tabla de ruteo. Para pasar los paquetes entre puertos, se utiliza la estructura de conmutación basada en memoria compartida, bus común o conmutación de circuitos. De modo similar a los conmutadores LAN, los ruteadores de alto rendimiento tienen una unidad de procesamiento central que lleva a cabo tareas generales: construye la tabla de ruteo, almacena parámetros de configuración,

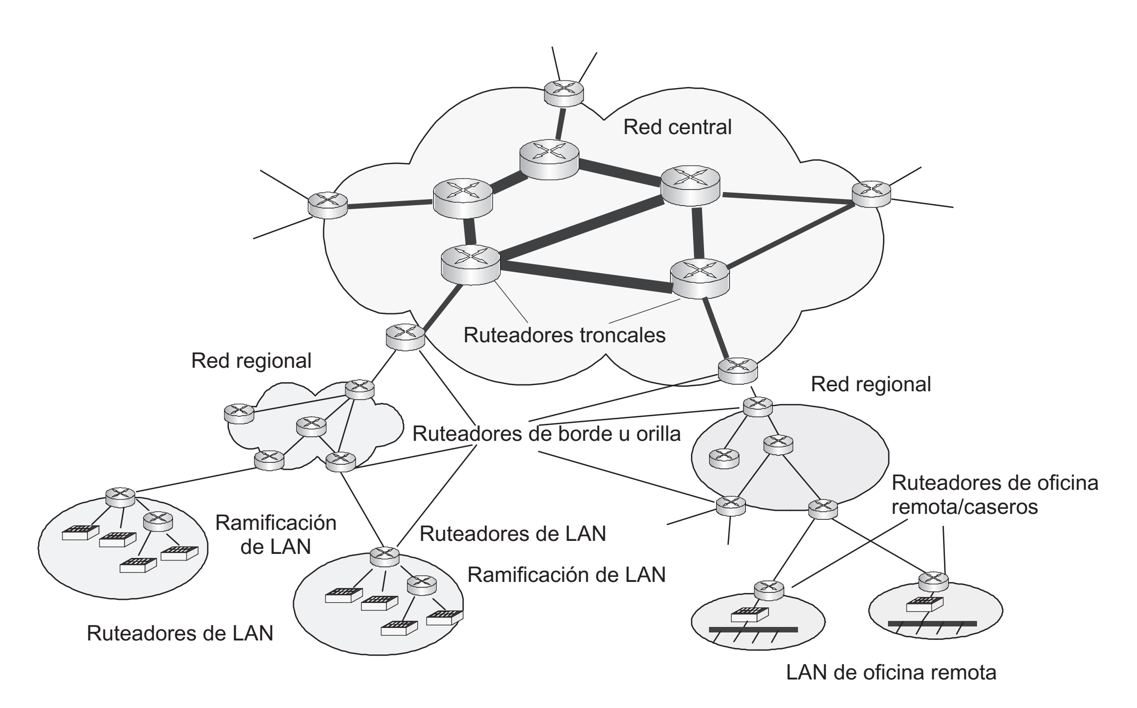


FIGURA 20.11 Tipos de ruteadores.

soporta la administración remota del ruteador y así sucesivamente. Dado que las funciones relacionadas con el envío de paquetes IP son significativamente más complicadas que el envío de la trama en las tecnologías LAN como Ethernet, la tarea de diseñar un puerto de alto rendimiento para el ruteador es bastante más complicada que la tarea similar para los conmutadores. Para hacer más simple y económico el procesador del puerto, los diseñadores suelen no cargarlo con funciones adicionales de ruteador, como el filtrado de tráfico o NAT. Incluso el soporte de QoS no siempre lo pone en marcha completamente un procesador así. Como regla, sólo se instalan mecanismos de cola, no así el perfil de tráfico. Esto se debe al ruteador troncal que funciona solamente dentro de la red y no interactúa con el mundo exterior, lo cual significa que no lleva a cabo funciones fronterizas que requieren perfilado y filtrado. La principal tarea de un ruteador de esta naturaleza consiste en pasar paquetes entre sus interfases a la máxima velocidad.

Un gran número de interfases permite construir topologías redundantes cercanas al diseño completamente conectado y así asegurar la tolerancia a fallas de la red. No obstante, el mismo ruteador fronterizo debe proporcionar alta confiabilidad. La tolerancia a las fallas y la confiabilidad del ruteador se consiguen a expensas de utilizar módulos redundantes tales como unidades de procesamiento central, procesadores de puerto y unidades de suministro de energía.

Los *ruteadores de orilla* o *borde* conectan el troncal a las redes periféricas y forman una capa especial que acepta el tráfico desde redes externas en relación con el troncal. Dichos ruteadores también se llaman *ruteadores de acceso*. La red periférica a menudo es administrada de manera autónoma. Ésta puede ser la red del cliente del portador de comunicaciones conectada directamente a su troncal o la red de un departamento regional de una empresa grande que tiene su propio troncal.

En cualquier caso, el tráfico llega a todas las interfases del ruteador fronterizo de la red que el administrador del troncal no puede controlar. Por lo tanto, debe filtrarse dicho tráfico y está sujeto a la política. Como resultado, los requerimientos para el ruteador de orilla son diferentes de aquellos para el ruteador troncal. Las capacidades del ruteador para asegurar máxima flexibilidad mediante la implementación y filtrado adicional de tráfico y funciones de política llegan al primer plano. Además, es importante asegurar que el rendimiento del ruteador fronterizo no es sacrificado por estas funciones adicionales. Las interfases del ruteador fronterizo no son tan rápidas como las del ruteador troncal. A pesar de ello, el ruteador fronterizo es más versátil, puesto que tiene que conectarse a las redes troncales basadas en tecnologías diferentes.

La división de ruteadores en troncales y de orilla no es estricta ni determinada. Una división así refleja simplemente el área de aplicación en la cual se prefiere usar el ruteador y donde sus ventajas son más evidentes. Cualquier ruteador puede emplearse fuera de su área principal de aplicación. Por ejemplo, el ruteador troncal equipado con puertos de alto rendimiento puede desempeñar el rol del ruteador de orilla simultáneamente. Un ruteador que lleva a cabo las tareas del ruteador fronterizo de una red grande y tiene esta función puede servir como ruteador troncal para una red más pequeña, donde sus interfases se las arreglarán con la carga sobre el troncal en una red de esta naturaleza.

Las diferencias principales de los **ruteadores portadores** de otros tipos de ruteadores son la alta confiabilidad y el soporte del conjunto completo de funciones requeridas para operación comercial como parte de internet, de BGP a los sistemas de control de los flujos de datos del usuario, que son requeridos para sistemas de facturación. Los altos requerimientos para confiabilidad se explican por el gran costo del tiempo de desactivación del ruteador cuando se proporcionan servicios comerciales. Los servicios de transmisión de datos aumentan constantemente; los usuarios de VPN e Internet quieren que estos servicios sean tan confiables como las comunicaciones telefónicas. Por lo tanto, cuando se establece que la disponibilidad de algunos ruteadores ha alcanzado la frontera de 0.999 y tiende al parámetro similar del equipo telefónico, el cual es de 0.99999, esto se relaciona principalmente con los ruteadores portadores tanto troncales como de orilla.

Los **ruteadores corporativos** tienen como finalidad usarlos dentro de los límites de una red corporativa; por consiguiente, los requerimientos de confiabilidad son menores que los de los ruteadores portadores. Además, los ruteadores corporativos no necesitan el conjunto completo de funcionalidad requeridos para funcionar como un sistema autónomo, que es parte de Internet.

Desde luego, las características de los ruteadores portadores y corporativos dependen significativamente de la escala de la corporación o portador de comunicaciones, además de sus características específicas. En la actualidad, un portador de comunicaciones internacionales que se relaciona con Tier 1 en la jerarquía ISP requiere ruteadores troncales equipados con interfases de 10 Gbps. Se espera que tales ruteadores sean remplazados pronto por ruteadores equipados con puertos DWDM que funcionan con 40 señales de onda y aseguran la tasa global de comunicaciones del puerto de 400 Gbps. Los ruteadores de orilla de un portador de esa índole también se calificarán como modelos de última generación. Los ruteadores de esta clase tendrán puertos que aseguren tasas o velocidades de acceso de 622 Mbps a 2.5 Gbps.

Los portadores de comunicaciones más pequeños, como los regionales y locales, no necesitan ruteadores con este nivel de rendimiento pues la cantidad total de su tráfico es significativamente inferior. Por lo tanto, el ruteador troncal de un portador así puede estar limitado al soportar interfases de 2 Mbps – 155 Mbps, y el ruteador de orilla debe asegurar el acceso por marcación de los suscriptores que usan líneas telefónicas. En redes pequeñas,

puede no haber ruteadores troncales, porque tales redes por lo regular abarcan uno o más ruteadores de orilla.

Una situación similar existe para las redes corporativas, en las que puede haber ruteadores con diferentes niveles de confiabilidad y rendimiento. Por ejemplo, las grandes corporaciones pueden utilizar ruteadores troncales y de orilla con características cercanas a las de los ruteadores propiedad de los portadores de comunicaciones Tier 1. No obstante, las redes corporativas por lo regular se basan en equipo con características que están en un nivel inferior. Esto significa que las grandes corporaciones utilizan equipo similar al empleado por portadores de comunicaciones regionales, y así sucesivamente.

Los **ruteadores departamentales** conectan departamentos regionales entre sí y a la red central. La red de un departamento regional, semejante a la red central, puede incluir varias LAN. Un ruteador así suele ser una versión algo similar de un ruteador troncal corporativo.

Si se construye un ruteador departamental en la base de un chasis, el número de ranuras en su chasis será de 4 a 5. También es posible diseñar un número fijo de puertos. Las interfases soportadas del LAN y WAN tienen velocidades inferiores a las correspondientes en los ruteadores corporativos. Esta clase de ruteadores liberados es la más grande, cuyas características pueden abarcar desde los cercanos a los ruteadores troncales hasta los que disminuyeron hasta ruteadores de oficina remota.

Los **ruteadores de oficina remota** conectan la única LAN de una oficina remota a la red central o a la red de un departamento regional en la que se emplea un enlace WAN.

Como regla, una interfase LAN es una Ethernet 10/100 Mbps, mientras que una interfase WAN es la línea rentada que asegura velocidades de 64 Kbps, 1 544 Mbps o 2 Mps. Un ruteador de oficina remota podrá soportar la operación si utiliza una línea telefónica de marcación como un enlace de reserva para la línea rentada. Existen muchos tipos de ruteadores de oficina remota, debido a que los clientes potenciales son numerosos y hay una gran variedad de aplicaciones para tales dispositivos. Esto puede explicarse tanto por un carácter masivo de clientes potenciales como por la especialización de este tipo de dispositivos, algunos de los cuales se han diseñado para soportar un tipo específico de comunicaciones de larga distancia. Por ejemplo, existen ruteadores que funcionan solamente en redes ISDN, así como algunos modelos están destinados sólo para líneas rentadas analógicas, y así sucesivamente.

Cuanto menores sean los requisitos para el rendimiento del ruteador, más alta será la probabilidad de que esté ideado de acuerdo con el diseño clásico de los primeros ruteadores (y puentes) de las LAN; es decir, con base en una sola unidad de procesamiento central y puertos que no tengan procesadores dedicados. Este diseño es considerablemente más económico, pero su desempeño depende en su totalidad del rendimiento del procesador y no puede ser escalado con un aumento del número de puertos.

El **ruteador de software** es un módulo de software especial de algún sistema operativo de propósito general, ya sea de la familia Windows o de UNIX.

Solamente el advenimiento de tecnologías de alta velocidad como ATM, SONET/SDH y DWDM incrementó de manera considerable los requisitos de rendimiento para los ruteadores. Como resultado, los representantes de la clase más avanzada de ruteadores han optado

por hacer diseños de multiprocesador con estructura de conmutación, lo cual se probó con éxito en conmutadores LAN.

> Los **ruteadores de LAN** (conmutadores de capa 3) están destinados a dividir grandes LAN en subredes. Esto es una clase especial de ruteadores que por lo regular no tienen interfases WAN.

Muchos ruteadores de esa clase se originaron de los conmutadores LAN, a los que dieron su nombre: conmutadores de capa 3, los cuales llevan a cabo todas las funciones del ruteador y además pueden funcionar como conmutadores LAN normales (es decir, conmutadores de capa 2). El modo de operación (conmutador o ruteador) depende de los parámetros de configuración.

Tales dispositivos también pueden funcionar en el modo combinado, en el que varios puertos del conmutador de capa 2 tienen la misma dirección IP (figura 20.12). En este caso, la transmisión de paquetes entre un grupo de puertos pertenecientes a la misma red se realiza en el modo de conmutación en la capa de enlace de datos (por ejemplo, basados en las direcciones MAC). Si los puertos pertenecen a diferentes redes IP, el conmutador llevará a cabo el enrutamiento entre redes. La selección del modo de transmisión del paquete está determinada por la configuración de las direcciones IP de los puertos y, en consecuencia, por la configuración de las computadoras.

EJEMPLO *Si dos computadoras (C1 y C2 en la figura 20.12) tienen direcciones pertenecientes a la misma red, cuando intercambien información no pasarán paquetes al ruteador predeterminado. En su lugar, utilizarán ARP para detectar la dirección MAC de la computadora de destino. Supóngase que la computadora C1 necesita pasar el paquete a la computadora C2. El conmutador de capa 3 pasa la trama de solicitud ARP*

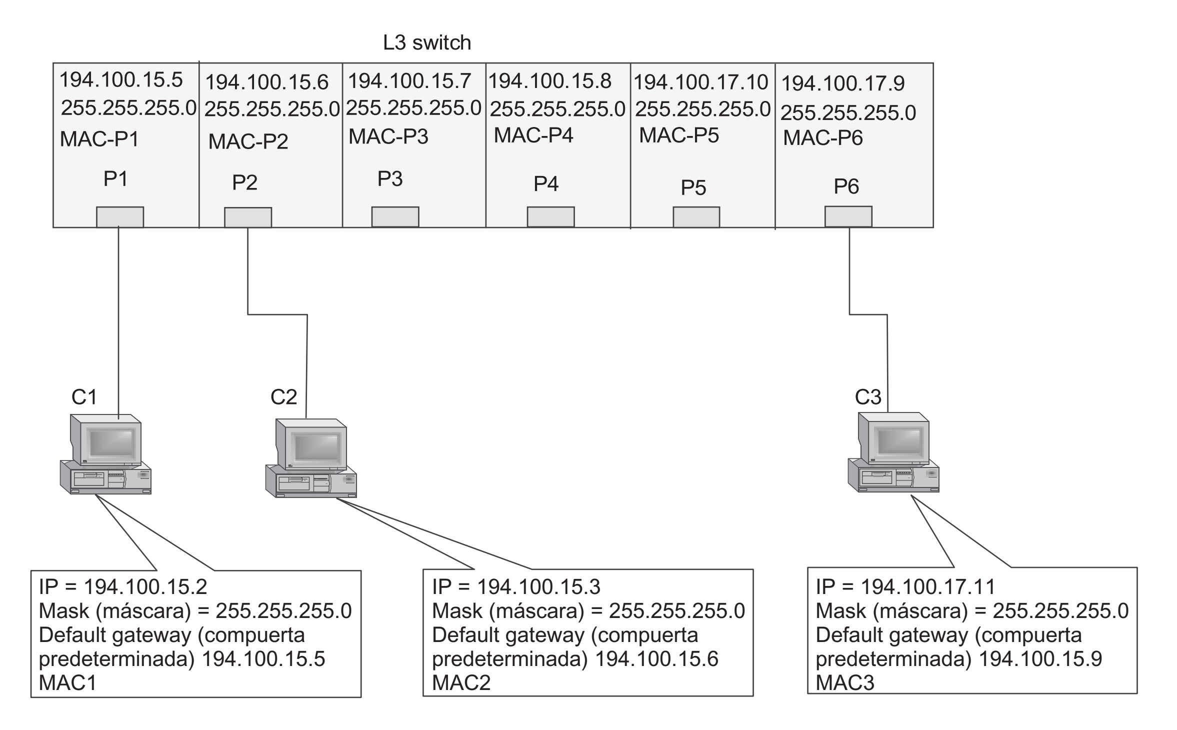


FIGURA 20.12 Modo de operación combinada del conmutador de capa 3.

con la dirección MAC de transmisión desde la computadora C1 a todos los puertos pertenecientes a la misma red IP (por ejemplo, a los puertos P1, P2, P3 y P4). La computadora C2 reconoce su dirección IP (194.100.15.3) en esta solicitud, responde al enviar la trama a la dirección MAC de destino de la computadora C1 (MAC1) y transporta información acerca de su propia dirección MAC (MAC2). Después de ello, la computadora C1 envía el paquete IP hacia la computadora C2, encapsulada en la trama con la dirección de destino MAC2. El conmutador de capa 3 pasa esta trama desde el puerto P1 hasta el puerto P2, de acuerdo con el algoritmo de puente, con base en la tabla de envío de capa 2. El conmutador de capa 3 funcionará de manera similar.

Cuando las computadoras pertenecen a diferentes redes IP, el comportamiento de la computadora emisora dicta el método de envío de paquetes al conmutador de capa 3. Por ejemplo, si la computadora C1 envía un paquete a la computadora C3, que se encuentra localizada en una subred diferente, deberá pasar el paquete al ruteador predeterminado en vez de intentar hallar la dirección MAC de la computadora de destino utilizando ARP. Por lo tanto, la computadora C1 envía la solicitud ARP para obtener la dirección MAC del ruteador predeterminado conocido. En el presente caso, es el puerto P1, que tiene la dirección IP IP-R1. Una vez que ha recibido la dirección MAC del puerto P1 (MAC-P1,) la computadora C1 envía el paquete IP destinado a la computadora C3 (es decir, con la dirección de destino 194.100.17.11) a ese puerto. Este paquete IP es encapsulado en la trama Ethernet con la dirección de destino MAC-P1. En cuanto ha recibido la trama con su dirección MAC, el conmutador de capa 3 la procesa de acuerdo con el método de enrutamiento en lugar del método de conmutación.

Los conmutadores de capa 3 soportan la técnica VLAN, que es el principal tipo de dispositivo para conectar VLAN separadas en una interred IP. Por lo regular, a cada VLAN se le asigna un número de red IP de modo que la transmisión de paquetes dentro de la VLAN se base en direcciones MAC y la transmisión de datos entre las VLAN esté basada en direcciones IP. En el ejemplo mostrado en la figura 20.12, los puertos P1-P4 pueden pertenecer a VLAN1, mientras que los puertos P5 y P6 corresponden a VLAN2.

RESUMEN

- ► Los ruteadores IP permiten el filtrado del tráfico del usuario con base en los atributos que incluyen las direcciones de origen y de destino, el tipo de protocolo conducido en los paquetes IP y los números de puerto UDP/TCP. Esta propiedad de los ruteadores se usa ampliamente para proteger las redes contra los ataques y para limitar el acceso de los usuarios legales.
- ► El filtrado de los anuncios de ruta asegura el control de la conectividad de la red como un todo y evita que aparezcan registros acerca de enlaces específicos en las tablas de ruteo.
- ► Los ruteadores IP han soportado mucho tiempo varios mecanismos de QoS, incluidas colas ponderadas y de prioridad, políticas de tráfico y retroalimentación para tráfico TCP. No obstante, sólo a mediados de la década de 1990 comenzó la investigación en el campo del desarrollo del sistema de los estándares de QoS IP, cuando fue necesario transmitir tráfico sensible al retardo sobre Internet.
- ► Actualmente existen dos sistemas de estándares QoS IP, IntServ y DiffServ. El primer sistema asegura calidad garantizada para microflujos y utiliza el protocolo de señalización

RSVP para reservar los recursos del ruteador de extremo a extremo. La desventaja del enfoque de IntServ es la carrera significativa sobre los ruteadores troncales, que deben almacenar información relacionada con el estado de millares de flujos de usuario.

- La tecnología DiffServ usa un enfoque agregado en el que la QoS está asegurada para mínimas clases de tráfico. Esto reduce significativamente la carga sobre los ruteadores; además, DiffServ está basada en el modelo de comportamiento per hop en el cual cada ruteador decide cuáles recursos debe dedicar a cada clase. Esto también simplifica la operación de los ruteadores, permite a cada ruteador decidir qué recursos debe asignar a cada clase de tráfico y facilita poner en práctica DiffServ en una red del proveedor. A pesar de ello, el enfoque DiffServ simplificado reduce el nivel garantizado de QoS, es decir, incrementa la probabilidad de que a veces la QoS exceda los límites requeridos por el cliente.
- Un ruteador típico es un dispositivo programable de cómputo que funciona bajo el control de un SO especializado optimizado para llevar a cabo las operaciones de construir tablas de ruteo y enviar paquetes
- Un ruteador se construye a menudo sobre el diseño de multiprocesador. Con más frecuencia, se utilizan el multiprocesamiento simétrico, el multiprocesamiento asimétrico o una combinación de ambos. La mayoría de las operaciones de rutina relacionadas con el procesamiento de paquetes se lleva a cabo programáticamente al emplear procesadores especializados o instalados a nivel del hardware (LIC/ASIC). Las acciones de un nivel superior se realizan de manera programática mediante procesadores universales.
- Para clasificar los ruteadores se pueden utilizar métodos diferentes: se pueden dividir en ruteadores troncales y de orilla (por sus posiciones relacionadas con la frontera de la red) y en ruteadores portadores y corporativos (según el tipo de compañía que posee la red). Los ruteadores que funcionan en redes empresariales extendidas se dividen por lo regular en ruteadores corporativos (aquellos que funcionan en la red central de la compañía), ruteadores de departamento regional y ruteadores de oficina remota. También existe una clase especializada de ruteadores destinada para las LAN, los cuales no soportan interfases WAN y por lo común se llaman *conmutadores de capa 3*.
- La tecnología de traducción de dirección de red (NAT) permite a una compañía resolver la escasez de direcciones IP y mejorar la seguridad de la red al ocultar las direcciones de los hosts. Esto se consigue al utilizar direcciones privadas en la red interna. Cuando el paquete deja los límites de la red interna, las direcciones privadas se traducen en direcciones IP globales.
- La NAT tradicional se subdivide tradicionalmente en la tecnología nata básica que usa sólo direcciones IP para mapeo y en la tecnología de traducción del puerto de la dirección de la red (NAPT, por sus siglas en inglés), en la cual los denominados identificadores de transporte también se emplean para traducción. Con mucha frecuencia, se utilizan los números de puerto TCP/UDP para este propósito.

PREGUNTAS DE REPASO

1. ¿Qué parámetros del paquete pueden utilizarse cuando se filtra tráfico en el ruteador?
   a) Dirección IP de origen
   b) Protocolo conducido en el paquete IP
   c) Número de puerto UDP/TCP
   d) Dirección IP de origen del paquete anterior

2. ¿Cuál es la diferencia entre los anuncios de ruteo y los resultados de filtrar el tráfico del usuario?
3. ¿Cuál es el significado de la palabra *integrada* en el nombre de la tecnología IntServ?
4. ¿Qué parámetros hacen posible limitar la ráfaga del flujo de paquetes de entrada perfilados al usar el algoritmo de cubeta de estafetas?
5. ¿Por qué la probabilidad de descartar paquetes en el método de detección aleatoria temprana (RED, por sus siglas en inglés) depende de la longitud promediada de la cola, más que de la longitud actual de ésta?
6. ¿Por qué el mecanismo RED no es aplicable al tráfico UDP?
7. Explique las etapas principales de la reservación de recursos del ruteador al emplear RSVP.
8. ¿Cuál es la limitación principal de la tecnología IntServ?
   a) No puede aplicarse al direccionamiento multidirigido
   b) El ruteador debe almacenar información acerca del estado de cada enlace
   c) Los nodos terminales deben actualizar periódicamente la reservación
9. ¿Por qué la tecnología DiffServ no utiliza un protocolo de señalización?
10. ¿Cuál es la diferencia entre los servicios EF y AF?
11. ¿Qué características específicas de la tecnología DiffServ la hacen popular entre los portadores de comunicaciones?
   a) Puede ponerse en práctica dentro de los límites de la red del portador de comunicaciones, independientemente de las redes de otros portadores de comunicaciones
   b) Los ruteadores funcionan con clases de tráfico, lo cual no crea una carga significativa sobre ellos
   c) Asegura la automatización de los cálculos de QoS
12. ¿Cuál es el objetivo principal de la NAT?
   a) Frustrar los ataques de DoS
   b) Resolver el problema de escasez de direcciones IP en IPv4
   c) Proteger el espacio de dirección interno de la compañía
13. ¿Qué atributos adicionales de paquetes se utilizan en NAT para mapear el conjunto de direcciones internas a una sola dirección global?
14. Rellene la columna del "puerto designado" de la tabla NAT.

Dirección privada	Puerto del emisor o remitente	Dirección global	Puerto designado
10.0.25.1	1035	193.55.13.79	
10.0.25.2	1035	193.55.13.79	
10.0.25.3	1035	193.55.13.79	
10.0.25.2	1047	193.55.13.79	
10.0.25.2	1047	193.55.13.79	

15. Liste las principales variantes de arquitectura del ruteador.
16. ¿Cuáles son los criterios empleados para clasificar ruteadores?
17. ¿Cuáles son las características específicas de los conmutadores de capa 3?

PROBLEMAS

1. Redacte una lista o listas de acceso para un ruteador Cisco que conecta la compañía a Internet (figura 20.13). La lista de acceso debe asegurar lo siguiente:
   a) Las comunicaciones de usuarios de la red 194.100.12.0/24, excepto para el usuario 194.100.12.25, con sólo los nodos de redes 132.22.0.0/16 y 201.17.200.0/24. Estos usuarios no deben intercambiar información con Internet.
   b) Debe proporcionarse al usuario 194.100.12.25 la posibilidad de intercambio ilimitado de datos.
   c) Los servidores de la red 201.17.200.0/24 deben estar accesibles desde Internet solamente al utilizar ftp y http. El acceso a estos servidores al usar ICMP debe denegarse.
2. Cuando se describe la tecnología NAT, se simplifica el patrón. En particular, no se consideran los problemas que pueden surgir cuando lleguen mensajes de error ICMP en la red interna. Sugiera su propia variante en el algoritmo que debería emplearse por el protocolo NAT cuando llegue un mensaje ICMP a su interfase externa.

CONSEJO *Antes de pasar el mensaje ICMP, ICMP debe introducir correcciones no sólo en el encabezado IP, sino también en el campo de datos ICMP.*

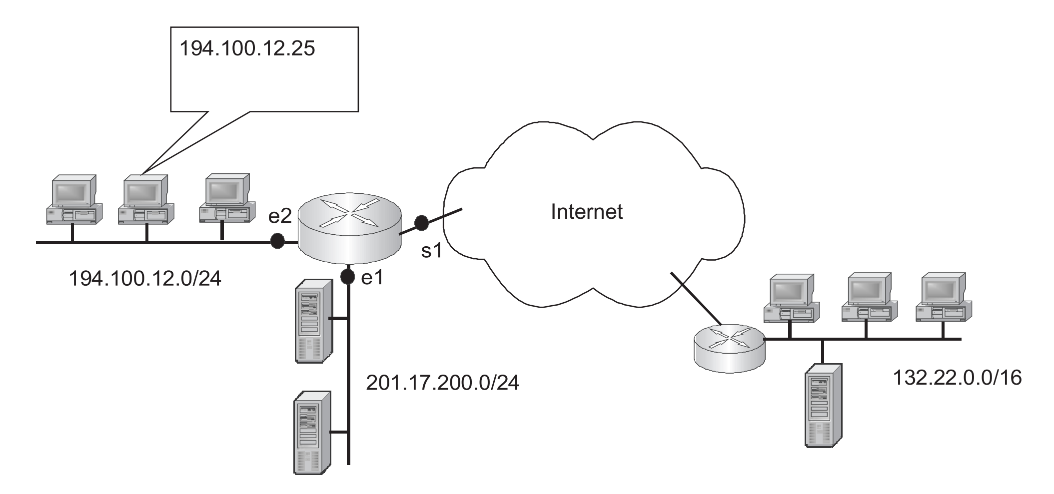


FIGURA 20.13 Filtrado del tráfico en el que se utiliza un ruteador.

PARTE **V**

REDES DE ÁREA AMPLIA

La tecnología IP considerada en la parte anterior del libro permite construir varios tipos de interredes, tanto LAN como WAN. Aparte de IP, existen otras tecnologías diseñadas de manera especial para construir WAN. Hay redes X.25, interesantes sólo desde el punto de vista histórico, así como también redes Frame Relay y ATM utilizadas ampliamente en la actualidad. Estas tecnologías tienen una característica en común: están basadas en la técnica de circuito virtual. Como se mencionó en la parte I, dicha técnica es una alternativa al método de datagramas de envío de paquetes en el que se basan las redes Ethernet e IP. La competencia entre estos dos principios de transmisión de datos ha existido desde el advenimiento de las primeras redes de paquetes conmutados.

A partir de la revolución de Internet, las WAN comerciales han dado preferencia a la técnica del circuito virtual. La justificación principal para este enfoque es que, en comparación con el método de datagrama de envío de paquetes, esta técnica asegura un nivel de control considerablemente superior sobre las conexiones entre usuarios de red y sobre las rutas a lo largo de las cuales viaja el flujo de información entre los nodos de red. Como resultado, el portador de comunicaciones puede controlar racionalmente la distribución de recursos entre los servicios a los cuales se han suscrito los usuarios. El problema de asegurar la QoS también puede resolverse con más facilidad cuando se utilizan circuitos virtuales. Desde luego, este enfoque no está libre de desventajas, principalmente los gastos significativos (tanto en tiempo como en dinero) para establecer cada conexión virtual. Por el contrario, el método de datagrama de comunicación entre nodos de red se distingue por la simplicidad de conectar cualquier nodo de red a cualquier otro nodo. No obstante, eso limita las capacidades del operador para controlar la distribución de recursos entre los usuarios. En las redes contemporáneas es posible hallar un compromiso al combinar ambos métodos. En las interredes que abarcan WAN, la mayoría de las redes constituyentes funcionan con base en la técnica de circuito virtual, lo cual significa que éstas son redes Frame Relay y ATM. Dichas redes están interconectadas con base en el protocolo de datagrama IP. Un enfoque de capas múltiples de esta naturaleza para construir WAN produce el resultado deseado, pero la organización WAN llega a ser demasiado complicada; además, algunas de sus funciones son parcialmente duplicadas. Por ejemplo, los protocolos de ruteo funcionan en redes ATM y en la capa IP.

Los intentos para conseguir la integración más estrecha entre el método de datagrama y el método de circuito virtual han conducido a diseñar la tecnología de conmutación de etiqueta de protocolo múltiple (MPLS, MultiProtocol Label Switching). MPLS utiliza ruteo de los protocolos de la pila TCP/IP para investigar la topología de la red y encontrar rutas racionales. A pesar de ello, envía paquetes de acuerdo con la técnica del circuito virtual.

Asegurar el acceso de alta velocidad a la red troncal es un problema urgente. Es necesario incrementar la tasa de acceso en miles de millones de enlaces de acceso mediante la conexión de las premisas del usuario a la oficina central más cercana del portador de comunicaciones. Por lo tanto, las soluciones troncales tradicionales, basadas sobre todo en fibra óptica y que requieren instalar nuevos cables, a menudo son económicamente ineficaces para proporcionar el acceso a la mayoría de los usuarios domésticos. Las tecnologías que utilizan la infraestructura de cable existente, como una línea de suscriptor digital asimétrica (ADSL), y funcionan según ciclos locales de la red telefónica existente, o módems de cable que emplean redes de TV por cable, son más eficaces. El acceso inalámbrico fijo o móvil es una solución alternativa.

En el presente texto sólo se abordarán las características fundamentales de las redes de área amplia, en particular de circuitos virtuales.

21

WAN DE CIRCUITO VIRTUAL

DESCRIPCIÓN DEL CAPÍTULO

21.1 INTRODUCCIÓN

Las tecnologías WAN tales como X.25, Frame Relay y ATM difieren considerablemente en sus características funcionales. Al mismo tiempo, todas utilizan una técnica de circuito virtual que es una variante de comunicación orientada a conexiones. En el *capítulo 3* se examinaron las características generales de este mecanismo. Ahora se analizarán los detalles de su implementación y las características específicas típicas para cada una de las tecnologías enumeradas.

Las tecnologías de circuito virtual se examinarán de manera cronológica. La tecnología X.25 apareció al inicio de la era de las redes de computadoras, prácticamente de manera simultánea con el proyecto ARPANET que llegó a ser el origen de Internet y el protocolo de datagrama IP. Las redes X.25 emplean circuitos virtuales para una transmisión de datos confiables, lo cual fue de primordial importancia en las décadas de 1970 y 1980 cuando esta tecnología llegó a ser extremadamente popular. Esto se debe a que muchos enlaces de esa época eran enlaces de comunicaciones analógicas que no podían asegurar de forma automática la transmisión confiable de datos digitales. Por lo tanto, las capacidades de las redes X.25 para restablecer paquetes dañados o perdidos fueron muy valiosas en ese tiempo.

Como resultado del advenimiento de enlaces digitales rápidos y confiables a mediados de la década de 1980, las funciones X.25 relacionadas con asegurar la transmisión confiable de datos llegaron a ser redundantes. Esta revolución tecnológica condujo al desarrollo principalmente de la nueva tecnología WAN: Frame Relay. Esta tecnología desempeña el mismo papel en las WAN que el efectuado por Ethernet en las LAN: realiza sólo el mínimo conjunto de funciones requerido para entregar tramas hacia el nodo de destino. Deshacerse de muchas funciones innecesarias en el mundo de las telecomunicaciones contemporáneas no es la única diferencia de Frame Relay respecto a X.25. La tecnología más reciente también agregó una característica importante: el soporte de QoS para el tráfico elástico. Inicialmente, los diseñadores de los estándares de Frame Relay no planeaban incluir soporte para el tráfico sensible al retardo. Por consiguiente, el nivel de retardo y el "jitter" no están incluidos en la lista de parámetros garantizados a los usuarios. Empero, es posible la transmisión de voz de alta calidad en redes Frame Relay, a condición de que los switches o switches de la red soporten la priorización del tráfico.

La tecnología ATM proporciona un conjunto versátil e integrado de servicios de transporte para sus usuarios. En contraste con X.25 y Frame Relay, ATM fue designada inicialmente como la tecnología orientada a la transmisión de todos los tipos existentes de tráfico: datos de computadora, voz, vídeo, control de objetos, etc. El tamaño fijo y pequeño de la trama, que esta tecnología denomina *célula*, minimiza los retardos del tráfico en tiempo real. ATM también puede agregar circuitos virtuales separados en trayectorias virtuales, lo cual mejora su escalabilidad. No obstante, la gran calidad de los servicios proporcionados también requiere un alto precio, debido a que las redes ATM son técnicamente complejas y costosas. Otra razón que evita que ATM llegue a ser un transporte universal es la dificultad para procesar las células a velocidades de transmisión sumamente elevadas, como de 2.5 y 10 Gbps. A pesar de ello, ATM es popular y ninguna otra tecnología existente ha alcanzado características comparables de QoS e ingeniería de tráfico.

21.2 TÉCNICA DE CIRCUITOS VIRTUALES

PALABRAS CLAVE: circuito virtual, canal virtual conmutado/permanente, colección virtual conmutada/permanente, protocolo de señalización, tabla de conmutación, tabla de ruteo, establecimiento de llamada, identificador de canal virtual, flujo de datos a corto plazo, flujo de datos a largo plazo y flujo de tráfico agregado.

Existen dos tipos de circuitos virtuales:

- **Circuitos virtuales conmutados** (SVC, por las siglas para Switched Virtual Circuits). Los SVCs se crearon por iniciativa del nodo terminal de la red, en los que se utiliza un procedimiento automático.
- **Circuitos virtuales permanentes** (PVC, por Permanent Virtual Circuits). Los PVC se crearon con antelación mediante la configuración manual de conmutadores o switches de la red. Este procedimiento lo lleva a cabo el administrador de la red, posiblemente mediante el sistema de administración centralizado de la red y algún protocolo de control (con mucha frecuencia, este protocolo es un protocolo propietario).

Las abreviaturas como SVC/PVC suelen interpretarse también como *canal virtual conmutado/permanente (switched/permanent virtual channel)* o *conexión virtual conmutada/permanente (switched/permanent virtual connection).*

Para comenzar, considérese el proceso de crear un SVC.

21.2.1 Circuitos virtuales conmutados

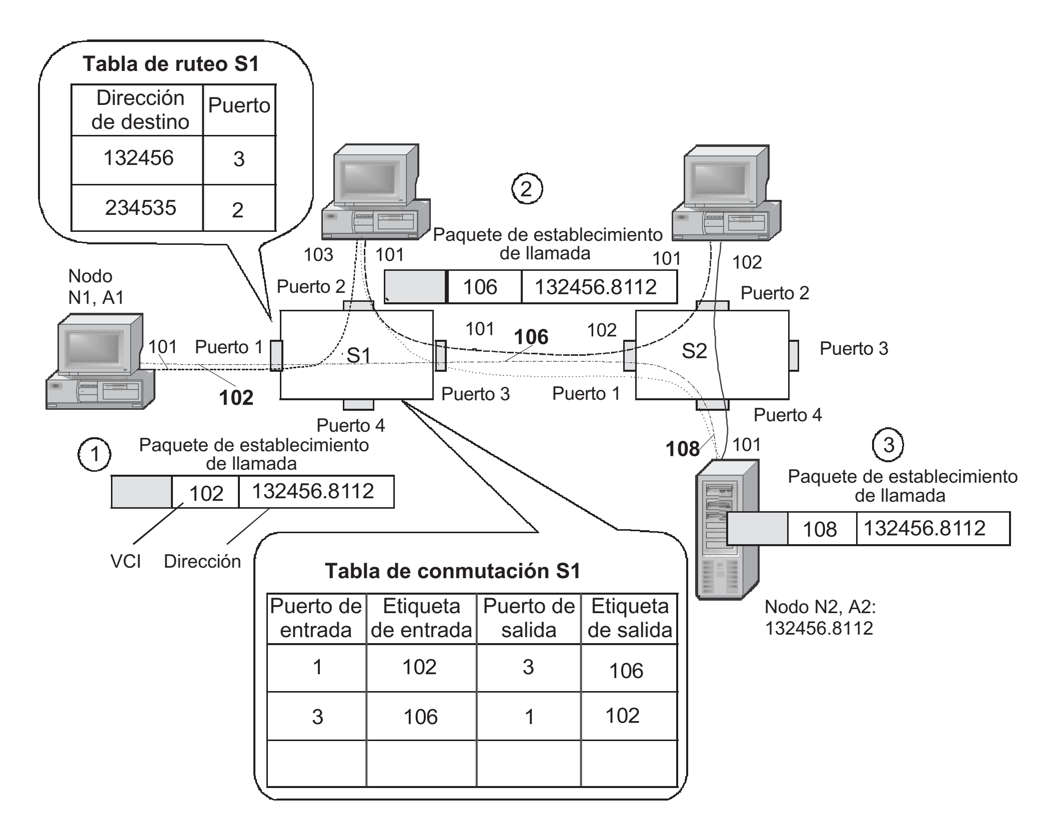
Los SVCs se crean mediante un procedimiento similar al empleado para establecer una conexión en redes telefónicas, el cual se examinó brevemente en el *capítulo 3*. En las redes telefónicas, el protocolo que pone en práctica un procedimiento así se conoce como **protocolo de señalización**. Por lo tanto, los protocolos utilizados para establecer un circuito virtual en redes de paquetes conmutados se reconocen a menudo mediante el mismo nombre.

La creación de un circuito virtual requiere tablas de ruteo semejantes a las utilizadas en redes de datagrama, como las redes IP, para estar presente en switches de red. El método empleado para crear tales tablas, ya sea manual o automático, no es importante. Un ejemplo de una tabla así se encuentra en la figura 21.1.

La figura 21.1 ilustra el proceso de creación de un circuito virtual en el que se conectan los nodos N1, A1 y N2, A2 a través de la red, que en este caso está representada por medio de dos switches: S1 y S2. La tabla de ruteo especifica la dirección de la red de destino. Este procedimiento tiene lugar en tres etapas, numeradas de acuerdo con la ilustración y la descripción que se proporcionan en seguida:

1. El procedimiento de creación de un circuito virtual comienza cuando el nodo de inicio (N1, A1) genera un paquete especial: una solicitud para establecer una colección lógica para el nodo N2, A2. En este ejemplo generalizado, dicha solicitud se conoce como **establecimiento de llamada** (el mismo término se utiliza en algunos protocolos de señalización específicos, como el Q.933 empleado con Frame Relay y el Q.2931 utilizado con ATM). Esta solicitud contiene un par de valores: la dirección del nodo de destino y el valor inicial del **identificador del canal virtual** (VCI, Virtual Channel Identifier). En este ejemplo, la solicitud inicial del establecimiento de llamada (Call Setup) tiene la forma siguiente:

   (102, 132456.8112)



Puerto de entrada	Etiqueta de entrada	Puerto de salida	Etiqueta de salida
1	102	3	106
3	106	1	102

FIGURA 21.1 Establecimiento de un circuito virtual

Aquí 102 es el valor inicial del VCI, mientras que 132456.8112 es la dirección de destino, donde la parte más significativa es el número de la subred y la parte menos significativa es el número del nodo.[1]

El número 102, asignado al circuito virtual, tiene el valor local para el puerto de la computadora a través de la cual se establece la conexión. Como ya existe un circuito virtual que pasa a través de este puerto (circuito número 101), el software del protocolo de señalización que se ejecuta en el nodo terminal ha seleccionado el primer número disponible (es decir, el número que no se encuentra en uso) del intervalo permitido. *Este enfoque garantiza la identificación unívoca de los circuitos virtuales dentro de cada puerto.*

El iniciador debe seleccionar el switch de red al cual es apropiado pasar la solicitud para establecer un circuito virtual. Esta selección puede estar basada en la tabla de ruteo del nodo remitente; no obstante, si el nodo se encuentra conectado a la red por medio de un puerto simple, como se ilustra en la figura 21.1, no será necesario tener una tabla de ruteo en el nodo terminal. Después de que el paquete de establecimiento de llamada llega al búfer del puerto 1 en el switch S1, se procesa de acuerdo con su dirección de destino y con los valores encontrados en la **tabla de ruteo**. El registro que conduce la dirección de la red de destino 132456 especifica que debe pasarse el paquete hacia el puerto 3.

[1] Este ejemplo utiliza direcciones de subred de 3 bytes y direcciones de nodo terminal de 2 bytes. En la práctica, las WAN basadas en circuitos virtuales emplean a menudo direcciones más extensas.

NOTA *Obsérvese que, en contraste con las tablas de ruteo de las redes IP, la tabla de ruteo proporcionada en la figura 21.1 no contiene información acerca de la dirección del siguiente switch. Esto se debe a que los switches WAN siempre están conectados mediante enlaces físicos de "punto a punto", los cuales no soportan conexiones múltiples. Por lo tanto, el número del puerto de salida identifica sin ambigüedad el switch siguiente.*

2. Después de determinar el número del puerto de salida para el paquete de establecimiento de llamada, el switch S1 genera el siguiente número VCI: 106. Este número fue seleccionado porque es el primer número disponible y dentro de los límites de esta sección local de la red identifica de manera unívoca el circuito virtual que se establece. Esta circunstancia se tuvo en cuenta al determinar al principio que los números VCI son *locales* por naturaleza. Después de cambiar el valor del VCI, el paquete de establecimiento de llamada toma la forma (106, 132456.8112) y es pasado a través del puerto de salida 3 del switch S1 hacia el puerto de entrada 1 del switch S2.

   De modo simultáneo al envío de paquetes, el switch crea la **tabla de conmutación** (no confundir con la tabla de ruteo mencionada anteriormente). Esta tabla se requerirá después, cuando se vaya a implementar el circuito virtual y los datos del usuario se transmitan a través de él, esta vez sin especificar la dirección de destino.

   Cada registro de la tabla de conmutación contiene cuatro campos principales:

   - Número del puerto de entrada
   - Etiqueta de entrada (VCI) en los paquetes que llegan al puerto de entrada
   - Número del puerto de salida
   - Etiqueta de salida (VCI) en los paquetes transmitidos a través del puerto de salida

   El registro "1-102-3-106" en la tabla de conmutación significa que todos los paquetes que llegan al puerto 1 y conducen VCI 102 se dirigirán hacia el puerto 3 y que el campo *VCI* se modificará a un nuevo valor: 106.

   Los circuitos virtuales pueden ser unidireccionales y bidireccionales. En el ejemplo considerado, el circuito es bidireccional; por lo tanto, el switch crea otro registro en la tabla de conmutación para el envío de paquetes en la dirección inversa desde el nodo N2, A2 hacia el nodo N1, A1. Este registro refleja al primero, de modo que el paquete con la etiqueta VCI 106 y que llega hacia el puerto 3 del switch S1 tendrá el valor inicial del VCI, 102, cuando deje el puerto 1. Como resultado, el nodo N1, A1 reconocerá correctamente el circuito virtual al que pertenece el paquete de llegada, a pesar de los constantes cambios de números en el curso de la transmisión del paquete a través de la red.

3. El conmutador o switch S2 continúa el procedimiento de establecer un circuito virtual. Para conseguir esto, emplea la dirección de destino especificada en la solicitud. El switch determina el puerto de salida al cual es necesario pasar el paquete, para lo cual utiliza su tabla de ruteo (no mostrada en la figura 21.1). De manera simultánea con esta operación, actualiza el campo *VCI*, en cuyo caso el switch tiene asignado el valor VCI 108 para el paquete de establecimiento de llamada. Como resultado, la solicitud de establecimiento de llamada llega al nodo de destino en la forma siguiente: (108, 132456.8112). Una vez que ha recibido la solicitud, el nodo terminal puede aceptarla o rechazarla. En caso de una decisión positiva, informará al iniciador acerca de su decisión al enviar el paquete de servicio *connect (conexión)*, el cual viaja a través de la red y utiliza registros "duplicados" en la tabla de conmutación. El paquete de conexión confirma el establecimiento de un circuito virtual a todos los switches y al iniciador.

Después de que el iniciador recibe el acuse de recibo de conexión, los nodos terminales pueden comenzar a utilizar este circuito virtual para enviar datos del usuario. Las células enviadas por el nodo terminal N1, A1 se dirigen con base en el VCI, el cual suele tener una longitud pequeña. Por ejemplo, en la tecnología X.25, su longitud es de 1.5 bytes solamente. Compárese esto con la longitud de dirección del nodo de destino, que en redes X.26 puede alcanzar los 16 bytes.

En principio, la técnica SVC utiliza dos métodos de operación de red:

- Cuando se establecen SVCs, las solicitudes para instalar una conexión se pasan a través de la red en la que se utiliza un modo de ruteo estándar. Este modo usa direcciones de destino, que son globales para toda la red, y requiere información completa acerca de la topología de la red. Esto significa que los protocolos para establecer circuitos virtuales (protocolos de señalización) funcionan en el nivel de la red del modelo OSI.
- Después de establecer una conexión, la red comienza a funcionar según las direcciones y tablas de direccionamiento locales, lo cual permite clasificar este modo como la capa de enlace de datos del modelo OSI. Los dispositivos de comunicaciones se clasifican como switches (éste es un nombre estándar para los dispositivos de dicho nivel).

21.2.2 Circuitos virtuales permanentes

El modo PVC no permite que los nodos terminales creen de manera dinámica circuitos virtuales. En vez de ello, el administrador de la red elabora previamente de forma manual las tablas de conmutación con antelación y puede llevar a cabo esta tarea en el ámbito local, por ejemplo, mediante conexión al switch utilizando la interfase RS-232 y empleando una computadora portátil como terminal virtual. Naturalmente, este método para configurar tablas de ruteo no es el más conveniente, en especial para sistemas distribuidos tales como las WANs. Por ende, como regla, los administradores confían en los sistemas de administración de red, los cuales se comunican con otros switches de la red al usar uno de los protocolos de administración, como pueden ser el de administración de red simple o el protocolo de información de administración común. El administrador suministra al sistema de administración de la red los datos de configuración y especifica a través de cuáles nodos debe pasar el circuito virtual que se crea. El sistema de administración de la red se comunica entonces con los switches de ésta mediante una selección automática de los valores referidos para las VCI y elabora registros en tablas de conmutación. Desafortunadamente, el uso de protocolos de administración de la red estándares no garantiza la compatibilidad entre los sistemas de administración de la red. Esto se debe a que tales sistemas son aplicaciones complejas puestas en práctica de manera diferente por diversos fabricantes.

En consecuencia, la automatización de los procedimientos para establecer PVC sólo es posible dentro de los límites de un segmento de red basado en equipo del mismo fabricante. A medida que se relaciona con los fragmentos PVC en las fronteras de la red, se deben “pegar” manualmente.

> Las tablas de ruteo son innecesarias cuando se crean PVC, pues la trayectoria es seleccionada por el administrador.

Con el fin de hacer utilizable el circuito virtual recién creado, el administrador debe introducir su número en los nodos terminales para los cuales se creó. Obsérvese que este número será diferente en ambas terminales. Por ejemplo, si el circuito virtual mostrado en la figura 21.1 se diseñara de manera permanente, el administrador de la computadora N1,

A1 tendría que introducir la etiqueta 102, y el administrador de la computadora N2, A2 la etiqueta 108.

Si la tecnología del circuito virtual soporta únicamente el modo PVC, éste permitirá a los usuarios considerarla una tecnología exclusivamente de capa de enlace de datos. Frame Relay es un buen ejemplo de una tecnología así, porque durante largo tiempo sólo el modo PVC existió en él. De este modo, su clasificación como tecnología de capa de enlace de datos estaba bien justificada. Aunque en la actualidad las redes Frame Relay soportan ambos modos, todavía se considera una tecnología de capa de enlace de datos con respecto al modo de direccionamiento de datos. En contraste con Frame Relay, la tecnología ATM ha soportado ambos tipos de circuitos virtuales desde que fue presentada. No obstante, también se clasifica a menudo como tecnología de capa 2 (Layer 2) por la misma razón.

21.2.3 Comparación con la técnica de datagrama

La técnica de los circuitos virtuales tiene sus ventajas y desventajas en comparación con la técnica de datagrama.

En contraste con los protocolos de datagrama, como IP, los protocolos de circuito virtual requieren que la conexión se establezca antes del intercambio de datos del usuario. Esto incluye un retardo adicional antes de iniciarse la transmisión de datos. Este retardo llega a ser especialmente notable cuando se transmite un pequeño volumen de datos, los denominados *flujos de datos a corto plazo*, porque el tiempo requerido para establecer el circuito virtual puede ser comparable con el tiempo de la transmisión de datos.

> Las redes de datagrama, donde no hay etapa de configuración de conexión, son más eficaces cuando transmiten *flujos de datos a corto plazo*. Las redes que soportan circuitos virtuales son más adecuadas para transmitir *flujos de datos a largo plazo*.

Sin embargo, tenga en cuenta que el tiempo gastado para establecer un circuito virtual se compensa por la transmisión más rápida de todo el flujo de paquetes. El ruteo en las redes que soportan la técnica de circuito virtual es más rápido debido a los dos factores:

- En primer lugar, la decisión de enviar un paquete específico se toma más rápido, porque las tablas de conmutación son más pequeñas.
- En segundo lugar, la cantidad de información de control en los paquetes es más pequeña. Las direcciones de los nodos terminales en WAN suelen ser bastante extensas; como regla, su longitud es de 14 a 15 dígitos decimales. En consecuencia, requieren hasta 20 bytes en el encabezado del paquete. En contraste con esta situación, el número del circuito virtual generalmente no excede de los 10 a 12 bits.

El modo PVC es el más eficaz desde el punto de vista del rendimiento. Una parte significativa del trabajo relacionado con el ruteo del paquete lo ha llevado a cabo el administrador de la red. En estas condiciones, los switches solamente tienen que enviar los paquetes con base en las tablas de conmutación creadas con anterioridad y lo hacen tan rápido como pueden. Un PVC es similar en muchos aspectos a una línea rentada porque no hay necesidad de establecer o terminar la conexión y el intercambio de paquetes puede iniciarse en cuanto sea necesario. La diferencia entre un PVC y una línea rentada es que el usuario no tiene garantías del ancho de banda del canal. La principal ventaja es que el uso de PVC resulta significativamente menos costoso que la renta de una línea, porque el usuario comparte el ancho de banda con otros usuarios de la red.

Los PVC son eficaces para transmitir **flujos de tráfico agregado** que abarca un gran número de flujos individuales de los suscriptores de la red. En este caso, el circuito virtual se crea en la sección troncal donde existe este flujo agregado. En lugar de usuarios finales, conecta dos dispositivos de borde, por ejemplo, los ruteadores fronterizos de dos portadores de comunicaciones. Debido a la ley de los grandes números, los flujos agregados se caracterizan por un alto nivel de estabilidad, de modo que no hay necesidad de crear SVC de manera dinámica. En estas condiciones, es mucho mejor utilizar de manera eficaz circuitos permanentes, los cuales se tardarán de modo suficiente en condiciones de buena planeación que utiliza ingeniería de tráfico.

Otra ventaja de las redes de datagrama reside en su rápida adaptación a los cambios topológicos ocasionados, por ejemplo, por una falla del enlace de comunicaciones o del ruteador. Cuando se presenta una situación así, los paquetes simplemente se envían por una nueva trayectoria. No obstante, en este caso es necesario tener en cuenta el retardo temporal para establecer una nueva configuración en las tablas de ruteo. Por otra parte, si falla el enlace de comunicaciones o uno de los ruteadores a lo largo de la trayectoria de un circuito virtual, la conexión se terminará y será necesario crear un nuevo circuito virtual que traspase las secciones fallidas de la red.

21.3 REDES X.25

PALABRAS CLAVE: interfase de usuario a red (UNI, User-to-Network Interface), interfase de red a red (NNI, Network-to-Network Interface), ensamblador-desensamblador de paquete (PAD, Packet Assembler-Disassembler), números internacionales de datos (IDNs, International Data Numbers), códigos de identificación de redes de datos (DNIC, Data Network Identification Codes), número terminal nacional, procedimiento balanceado de acceso de enlace (LAP-B, Link Access Procedure-Balanced) e interfases X.21 y X.21 bis.

21.3.1 Estructura y objetivos de las redes X.25

La recomendación X.25 ("interfase entre equipo de terminal de datos [DTE] y tipo de circuito de terminación de datos [DCE] para terminales que funcionan en el modo de paquetes y conectada a redes de datos públicas mediante circuitos dedicados"] fue diseñada por la CCITT (ahora conocida como ITU-T) en 1974. Desde entonces, ha sido revisada varias veces.

De acuerdo con su título, este estándar no describe la estructura interna de las redes X.25. Por el contrario, únicamente define la interfase del usuario con la típica red para las WAN. Esta interfase se conoce como **interfase del usuario a la red** (UNI, por sus siglas en inglés). La estructura interna de la red puede ser arbitraria y se elige a la discreción de los portadores de comunicaciones. En la práctica, los switches de WAN se comunican mediante protocolos similares al UNI. Para organizar las comunicaciones entre redes propiedad de diferentes portadores de comunicaciones, por lo regular es necesario elaborar una **interfase de red a red** (NNI), la cual suele ser una versión modificada de UNI.

La tecnología de la red X.25 tiene varias características importantes que la hacen significativamente distinta de otras tecnologías:

- X.25 es la más adecuada para transmitir el tráfico típico de baja intensidad para terminales que fueron muy populares en las décadas de 1970 y 1980, y menos apropiada para los requerimientos superiores del tráfico de la LAN.

- La presencia de un dispositivo especial, **el ensamblador-desensamblador de paquetes** (PAD, por sus siglas en inglés), destinado para ensamblar varios flujos de baja velocidad de byte de inicio-parada de terminales de caracteres a computadores para procesamiento. La presencia de los PAD da fecha a la tecnología X.25, pues a principios de la década de 1970 las terminales de caracteres eran dispositivos pasivos capaces de llevar a cabo sólo operaciones primitivas. Las otras operaciones relacionadas con las funciones de enlace de datos y funciones de capa de red se realizaban mediante PAD.
- La presencia de una pila de protocolo X.25 de tres capas en la que se utilizan protocolos orientados a la conexión para capa de enlace de datos y capa de red para controlar flujos de datos y corregir errores. Una redundancia de funciones de esta clase para asegurar la transmisión confiable de datos es provocada por la orientación de dicha tecnología hacia los enlaces de comunicaciones no confiables, que tenía una característica BER de 10^{-3} a 10^{-4}.
- La orientación hacia pilas uniformes de protocolos de transporte en todos los nodos de la red, debido a que la capa de red se ha diseñado para trabajar únicamente con el protocolo de capa de enlace de datos. En contraste con IP, no puede interconectar redes heterogéneas.

Una red X.25 consta de switches distribuidos geográficamente y conectados mediante enlaces rentados de alta velocidad (figura 21.2). Las líneas rentadas pueden ser tanto digitales como análogas.

Los PAD pueden ser remotos o interconstruidos. Como regla, un PAD interconstruido está montado en el estante o "rack" de switches. Las terminales tienen acceso al PAD interconstruido mediante líneas telefónicas con el uso de módems. Un PAD remoto es un dispositivo independiente pequeño conectado al switch por medio de un enlace X.25 dedicado. Las terminales están conectadas al PAD remoto mediante una interfase asincrónica. Como regla, se utiliza la interfase RS-232C para este propósito. Un PAD simple proporciona gene-

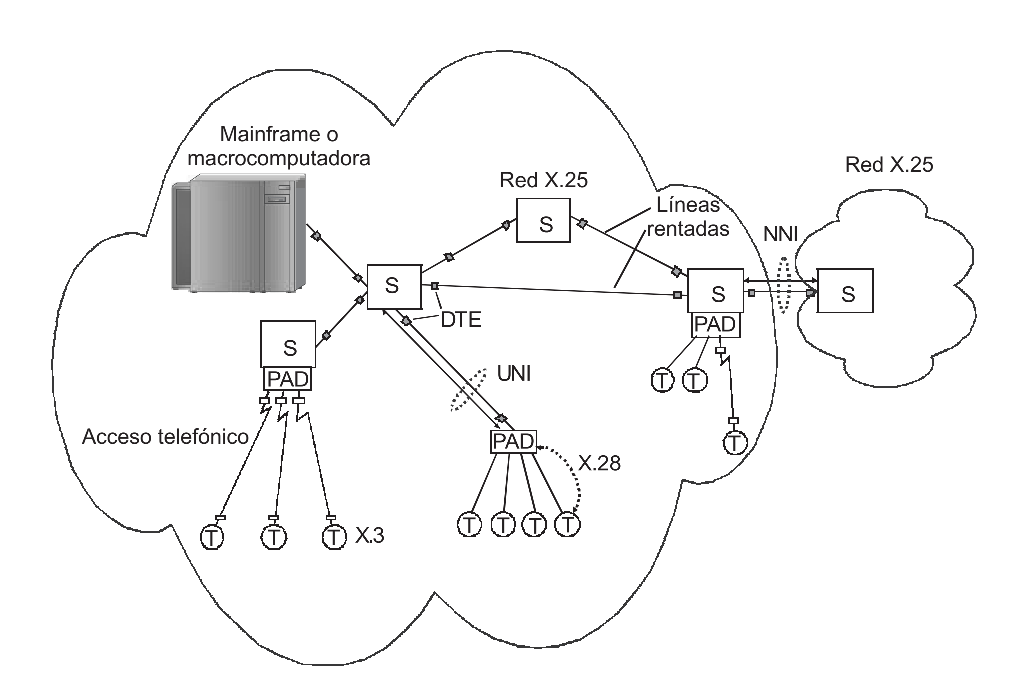


FIGURA 21.2 Estructura de la red X.25.

ralmente acceso para 8, 16 o 24 terminales asincrónicas. Las terminales no son direcciones de nodos terminales asignadas de la red X.25. Las direcciones se asignan a puertos PAD, que están conectados al switch del paquete X.25 al emplear un enlace rentado.

Las computadoras y LAN se encuentran conectadas directamente por lo regular a la red X.25 por medio de un adaptador X.25 o el ruteador que soporta los protocolos X.25 en sus interfases.

21.3.2 Direccionamiento en redes X.25

Si la red X.25 no tiene conexión al mundo exterior, puede utilizar direcciones de cualquier longitud (dentro de los límites implicados por el formato del campo de dirección) y asignar cualquier valor a las direcciones. La longitud máxima del campo de dirección en el paquete X.25 llega a 16 bytes.

La recomendación CCITT X.121 define un sistema internacional para la numeración de direcciones en las redes públicas de datos. Si una red X.25 necesita intercambiar datos con otras redes X.25, deberá cumplir con el estándar de direccionamiento X.121.

Las direcciones X.121, también conocidas como **números internacionales de datos** (IDN, por sus siglas en inglés), tienen longitudes diferentes que pueden alcanzar los 14 dígitos decimales.

- Los primeros cuatro números de la IDN son los **códigos de identificación de redes de datos** (DNIC, por sus siglas en inglés). La DNIC se encuentra dividida en dos partes:
  - La primera parte (tres dígitos decimales) define el país en el cual se localiza la red.
  - La segunda parte (un dígito decimal) es el número de la red X.25 dentro de ese país.

  De este modo, sólo 10 redes X.25 pueden organizarse dentro de cada país. Cuando es necesario tener más, se deben asignar varios códigos a ese país.
- Los otros dígitos establecen el **número terminal nacional** y permiten que un dispositivo DTE específico sea identificado dentro de la red X.25.

21.3.3 Pila de protocolos en redes X.25

Los estándares de las redes X.25 describen tres capas de protocolos (figura 21.3).

- En la *capa física* existen dos **interfases sincrónicas, X.21** y **X.21 bis**, para equipo de transmisión de datos: ya sea para DSU/CSU si el enlace rentado es digital, o para un módem sincrónico si es un enlace analógico. El protocolo de capa física del enlace de comunicaciones no está predefinido, lo que ofrece la posibilidad de utilizar enlaces correspondientes a diversos estándares.
- En la *capa de enlace de datos* se utiliza el **procedimiento balanceado de acceso de enlace (LAP-B, Link Access Procedure-Balanced)**, que asegura la posibilidad de retransmitir de forma automática en caso de errores en la línea. Este protocolo asegura un modo balanceado de operación, lo cual significa que ambos nodos participantes en la conexión son iguales. De acuerdo con LAP-B, la conexión se establece entre el DTE (computadora, ruteador IP o ruteador IPX) y el switch de la red. Aunque el estándar no lo establece explícitamente, LAP-B también se utiliza a menudo para establecer conexiones en la capa de enlace de datos entre switches de red conectados directamente. LAP-B es un protocolo orientado a conexión que usa el algoritmo de ventana deslizante para asegurar la transmisión confiable de tramas entre dos dispositivos conectados directamente. En contraste con

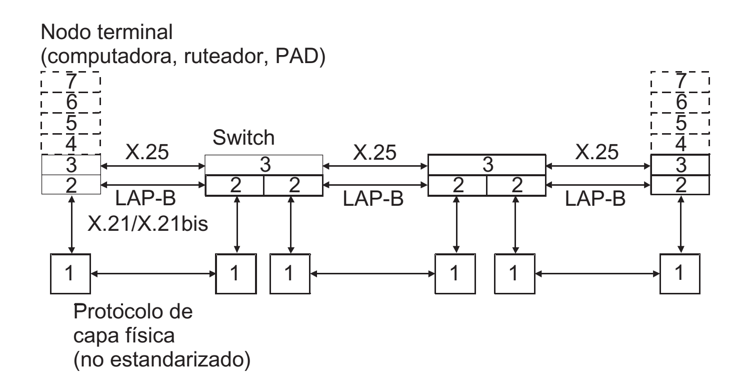


FIGURA 21.3 Pila de protocolo de una red X.25.

TCP, LAP-B emplea una implementación más simple de este algoritmo. En tal caso, las tramas transmitidas se enumeran como bytes en lugar de conjuntos. La ventana no puede cambiarse dinámicamente y tiene un tamaño fijo de 8 o 128 tramas. LAP-B pertenece a la familia de protocolos de control de enlace de datos de alto nivel (HDLC, High-level Data Link Control), la cual se examinará con más detalle en el *capítulo 22*.

- En la *capa de red* (el estándar utiliza el término *capa de paquete* en lugar del término *capa de red*), el estándar define el protocolo X.25/3 de intercambio de paquetes entre el equipo de la terminal y la red de transmisión de datos. Las conexiones LAP-B aseguran comunicaciones confiables entre un par de nodos NEIGHBOR (vecinos) pero no habilitan a los nodos END (terminales) para intercambiar información. Con el fin de establecer cierta conexión virtual terminal, se utiliza el protocolo X.25/3.

Considérese la operación del protocolo X.25/3 con más detalle. Sus principales funciones se enumeran a continuación:

- Enrutamiento de paquetes.
- Establecimiento y terminación de circuitos virtuales entre suscriptores de la red.
- Control de flujos de paquetes.

De acuerdo con este protocolo, el nodo terminal envía el paquete de *solicitud de llamada* (*call request*) encapsulado en la trama LAP-B.

NOTA *En contraste con otras redes basadas en la técnica del circuito virtual, las redes X.25 no utilizan un protocolo de señalización por separado. Cuando es necesario, el protocolo X.25/3 lleva a cabo esta función al conmutarse en un modo de operación especial.*

El paquete de *solicitud de llamada* especifica las direcciones de origen y destino en el formato X.121 y es recibido por el switch de la red y enrutado de acuerdo con la tabla de ruteo, con lo cual crea un circuito virtual. El protocolo de ruteo no está definido para las redes X.25; por lo tanto, las tablas de ruteo siempre se elaboran aquí en forma manual.

A medida que el paquete de solicitud de llamada (Call Request) viaja a lo largo de la ruta de switch en switch, los hace generar nuevos registros en tablas de conmutación y asignarles nuevos valores de etiqueta. De este modo, se crea un nuevo circuito virtual. El valor inicial del número del circuito virtual lo especifica el usuario en el campo del *número de canal lógico* (LCN, *Logical Channel Number*) de este paquete. Dicho campo es el análogo del campo *VCI* mencionado cuando se describió el principio del establecimiento de los circuitos virtuales.

Después de establecer un circuito virtual, los nodos terminales se intercambian con paquetes de otro formato: paquetes de *datos*. En estos paquetes, las direcciones de origen y destino no están especificadas y sólo la etiqueta *LCN* se queda con toda la información de la dirección.

La diferencia de la tecnología X.25 respecto a Frame Relay y ATM, que se examinará posteriormente en este capítulo, reside en la tecnología de capa de red. En realidad, después de que se establece un circuito virtual, la transmisión de datos se lleva a cabo mediante un protocolo de capa de red en vez de un protocolo de capa de enlace de datos.

21.4 REDES FRAME RELAY

PALABRAS CLAVE: tecnología ISDN, Frame Relay y Frame Switching, LAP-F (Q.922), núcleo LAP-F, control LAP-F, LAP-D (Q.921) y Q.933, identificador de conexión de enlace de datos (DLCI, Data Link Connection Identifier), C/R, DE, FECN и BECN, elegibilidad de rechazo (DE, Discard Elegibility), tasa de información dedicada (CIR, Committed Information Rate), tamaño de ráfaga dedicada (BC, Committed Burst size), tamaño de ráfaga en exceso (B_e) y QoS.

Frame Relay es una tecnología relativamente nueva mucho más adecuada para la transmisión del tráfico de ráfaga típico para redes de computadoras en comparación con las redes X.25. Esta ventaja es evidente sólo cuando la calidad de los enlaces de comunicaciones llega a ser comparable con la de los enlaces de comunicaciones de LAN. Como se relaciona con los enlaces WAN, tal calidad se obtendrá por lo regular sólo si se utilizan cables de fibra óptica.

Al principio, la tecnología Frame Relay fue estandarizada por CCITT como uno de los servicios de la red digital de servicios integrados (ISDN, Integrated Services Digital Network) (RFC 2955). La tecnología ISDN se diseñó primero para poner en práctica una red universal global en la que se proporcionaban todos los servicios de transmisión de datos y telefonía. Desafortunadamente, este ambicioso proyecto no alcanzó su meta inicial. Una red de siguiente generación se ha creado con base en otras tecnologías, como IPX. Sin embargo, varios objetivos no menos importantes se lograron al poner en marcha este proyecto. La lista de tales logros incluye el diseño de la tecnología Frame Relay, la cual ha llegado a ser una tecnología autónoma independiente de ISDN.

En las recomendaciones I.122 liberadas en 1988, este servicio fue enumerado como un agregado de servicios ISDN en modo de paquete. A pesar de ello, en 1992 y 1993, cuando se revisaron estas recomendaciones, se definieron dos nuevos servicios en los estándares: **Frame Relay** y **Frame Switching**. La diferencia entre estos dos servicios reside en que Frame Switching asegura una entrega de trama garantizada y Frame Relay, como ya se mencionó, sólo proporciona el servicio del mejor esfuerzo.

Sencilla pero eficaz para los enlaces de comunicaciones de fibra óptica, la tecnología Frame Relay atrajo de inmediato la atención de la mayoría de las organizaciones y portadores de telecomunicaciones involucrados en el proceso de estandarización. Aparte de la CCITT (ITU-T), existen otras organizaciones que participan activamente en la estandarización de esta tecnología. La lista de ellas incluye el Frame Relay Forum (FRF) y el comité ANSI T1S1. En la medida en que se relaciona con la tecnología Frame Switching, permanece como un estándar que no encontró un área amplia de aplicación.

Los estándares Frame Relay diseñados por ITU-T/ANSI y FRF definen dos tipos de circuitos virtuales: persistentes (PVC) y conmutados (SVC). Esto corresponde a las necesidades del usuario, pues los circuitos persistentes son más adecuados para conexiones que transmiten

tráfico de modo constante. Por otra parte, para las conexiones utilizadas prácticamente varias horas por mes, los SVC son más apropiados.

Sin embargo, los fabricantes de equipo Frame Relay y los proveedores de servicios de red Frame Relay comenzaron a dar soporte sólo a los PVC. Desde luego, ésta es una simplificación considerable de dicha tecnología. El equipo soporta la aparición de SVC en el mercado con un retardo significativo; por consiguiente, Frame Relay suele estar asociado sólo con PVCs.

21.4.1 Pila de protocolos de Frame Relay

La pila de protocolos Frame Relay está organizada de modo mucho más simple que la pila de la tecnología X.25. Los diseñadores de Frame Relay han tomado en cuenta la alta calidad de los enlaces de comunicaciones de fibra óptica, que aparecieron a finales de la década de 1980. Por lo tanto, consideraron posible no incluir las funciones de confiabilidad en los protocolos de la pila. Son poco probables los errores cuando se utilizan tales enlaces de comunicaciones. Si, a pesar de la baja probabilidad de error, todavía surge una situación así, Frame Relay la ignora y deja todas las funciones relacionadas con la recuperación de los paquetes perdidos o corrompidos a protocolos de capa superior, como TCP.

> Debido a la baja redundancia del protocolo, Frame Relay es capaz de asegurar un amplio ancho de banda y pocos retardos de trama.

NOTA *Al mismo tiempo que Frame Relay se diseñó la tecnología Frame Switching, la cual, de manera semejante a X.25, asegura una transmisión confiable de la trama en la capa de enlace de datos. Esta tecnología se puede utilizar cuando los enlaces de comunicación no son caracterizados mediante calidad satisfactoria o cuando se requiere la capa de enlace de datos para asegurar una transmisión confiable de la trama debido a algunas razones. No obstante, en la práctica, la tecnología Frame Switching no encontró una amplia aplicación. Sin embargo, se menciona brevemente aquí, debido a que al crear la pila de protocolo Frame Relay se tuvo en cuenta la existencia de esta tecnología.*

La figura 21.4 muestra la pila de protocolo Frame Relay y la Frame Switching tal como se describen en las recomendaciones ITU-T. Los protocolos del plano de control llevan a cabo todas las operaciones relacionadas con el establecimiento de una conexión virtual, y los protocolos del plano de datos transmiten las tramas mediante el uso del circuito virtual establecido.

El protocolo de *procedimiento de acceso de enlace para servicios del portador en modo de trama* (**LAP-F**, por sus siglas para *Link Access Procedure for Frame mode bearer services*), que en las recomendaciones ITU-T se denomina **Q.922**, funciona en la capa de enlace de datos de las redes Frame Relay. Existen dos versiones de este protocolo:

- El **núcleo LAP-F** es un caballo de batalla que trabaja en todas las redes Frame Relay. El núcleo LAP-F, que se marca en fondo gris en la figura 21.4, proporciona el conjunto mínimo de herramientas con base en las cuales es posible construir una red Frame Relay. Sin embargo, en este caso, una red así proporcionará únicamente servicios PVC.
- El protocolo de **control LAP-F**, que debe operar en la red si también proporciona servicios de Frame Switching.

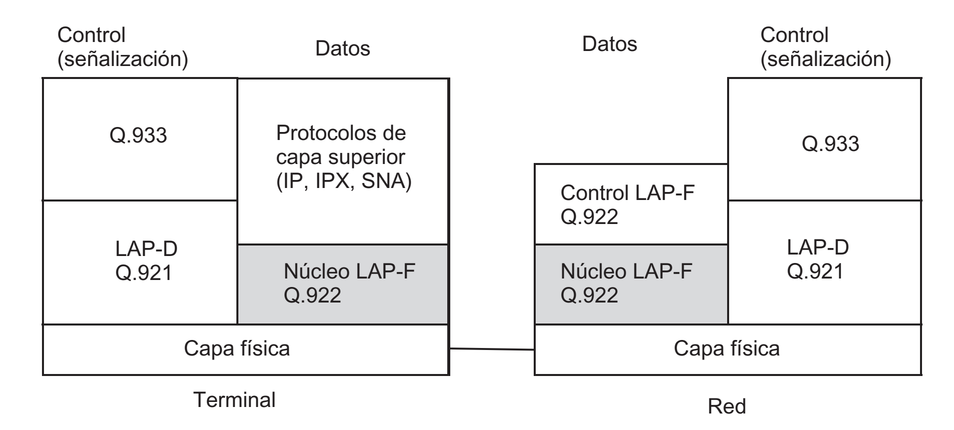


FIGURA 21.4 Pila de protocolos Frame Relay.

Tanto el núcleo LAP-F como el control LAP-F son protocolos de capa de enlace de datos que aseguran la transmisión de tramas entre switches vecinos.

En la *capa física*, una red Frame Relay puede utilizar enlaces PDH/SDH o enlaces ISDN.

Ahora considérese la capa de control que es responsable de establecer SVCs dinámicos. Para asegurar el modo SVC, los switches de red deben soportar dos protocolos de plano de control: el **procedimiento de acceso de enlace D** (LAP-D, Link Access Procedure D o **Q.921**) en la capa de enlace de datos y **Q.933** en la capa de red. El LAP-D en Frame Relay asegura la transmisión confiable de la trama entre switches vecinos.

El protocolo Q.933 utiliza direcciones del nodo terminal entre las cuales se establece un circuito virtual. Por lo regular estas direcciones están especificadas en el formato de número telefónico de acuerdo con el estándar E.164. Una dirección abarca 15 dígitos decimales, que, de modo similar a los números telefónicos normales, se encuentran divididos en un campo de *código de país* (1-3 dígitos), un campo de *código de ciudad* y un campo de *número de suscriptor*. La dirección ISDN incluye el número más la **subdirección** que puede abarcar hasta 40 dígitos. La subdirección se utiliza para dispositivos de terminal de numeración después de DTE, si el suscriptor tiene varios dispositivos de este tipo.

El protocolo para la creación automática de tablas de ruteo no está definido para la tecnología Frame Relay; por lo tanto, puede emplearse un protocolo propietario del fabricante del equipo. Como una alternativa, es posible crear de forma manual la tabla de ruteo.

NOTA *La principal ventaja que tiene la tecnología Frame Relay sobre la X.25 es que, después de establecer una conexión virtual, al transmitir las tramas se usa sólo el protocolo de capa de enlace de datos. En las redes X.25, los datos del usuario se transmiten mediante protocolos de capa de enlace de datos y de capa de red después de establecer una conexión. El uso de este enfoque permite que la tecnología Frame Relay reduzca el gasto extra para la transmisión de paquetes LAN, pues son encapsulados dentro de las tramas de capa de enlace de datos en lugar de paquetes de capa de red, como era el caso de las redes X.25.*

La tecnología Frame Relay se clasifica con mucha frecuencia como una tecnología de capa de enlace de datos, en la cual la atención principal se centra en los procedimientos de transmisión de datos del usuario. Los procedimientos para establecer un circuito virtual se llevan a cabo mediante el protocolo de capa de red.

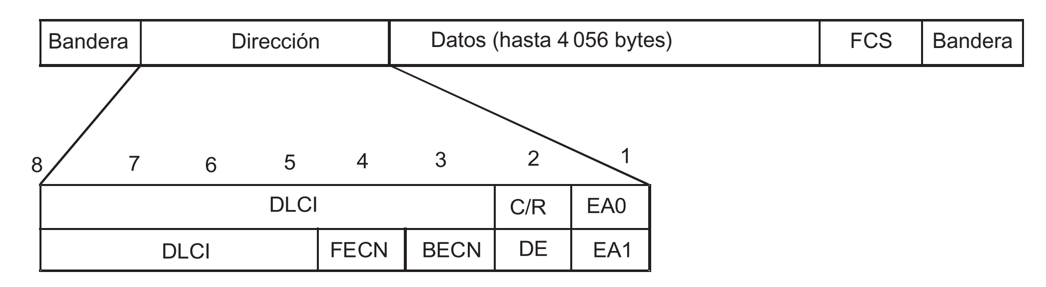


FIGURA 21.5 Formato de la trama LAP-F.

Los circuitos virtuales Frame Relay pueden utilizarse para transmitir datos de diferentes protocolos. La especificación RFC 1490 determina los métodos para encapsular los paquetes de protocolos de red como IP e IPX además de datos SNA en las tramas de Frame Relay.

La estructura de LAP-F se muestra en la figura 21.5.

El campo del **identificador de conexión de enlace de datos** (DLCI, Data Link Connection Identifier) ocupa 10 bits, lo cual permite usar hasta 1 024 conexiones virtuales. El campo *DLCI* puede ser más extenso; la longitud está controlada por los atributos EA0 y EA1 (aquí, EA significa dirección extendida, por sus siglas en inglés). Si el bit en este atributo se establece a cero, la bandera se conocerá como EA0 y especificará que el siguiente byte contiene la continuación del campo de dirección. Si esta bandera se establece a 1, el campo se denominará EA1 e indicará la terminación del campo de dirección.

Generalmente se utiliza el formato de 10 bits del campo *DLCI*. Sin embargo, cuando se utilizan 3 bytes para direccionamiento, el campo *DLCI* tiene 16 bits de largo, mientras que cuando se emplean 4 bytes, su longitud llega hasta los 23 bits.

Los estándares Frame Relay distribuyen direcciones DLCI entre usuarios y la red de la manera siguiente:

- 0: utilizada para el circuito virtual LMI.
- 1-15: reservadas para uso futuro.
- 16-991: usadas por suscriptores para numerar PVC y SVC.
- 992-1007: empleadas por servicios de transporte de red para conexiones de red internas.
- 1008-1022: reservadas para uso futuro.
- 1023: utilizada para controlar la capa de enlace de datos.

Así, en cualquier interfase Frame Relay, se asignan 976 direcciones DLCI para dispositivos de terminal de usuario.

El campo de datos puede tener un tamaño de hasta 4 056 bytes.

El campo C/R tiene el significado normal para dicho protocolo de la familia HDLC: éste es el atributo "comando-respuesta".

Los campos DE, FECN y BECN se emplean por el protocolo para controlar el tráfico y soportar la QoS especificada para un circuito virtual.

21.4.2 Soporte de QoS

Para cada conexión virtual, se definen varios parámetros, cada uno de los cuales se relaciona con la velocidad de transmisión de datos e influye en la QoS.

- **Tasa o velocidad de información dedicada (CIR, Committed Information Rate)**: velocidad de información confirmada a la cual la red transmitirá los datos del usuario.
- **Tamaño de la ráfaga dedicado (Bc)**: tamaño confirmado de la ráfaga (es decir, número máximo de bytes de este usuario) que la red transmitirá por intervalo de tiempo confirmado *T*, el cual se denomina **tiempo de ráfaga.**
- **Tamaño de la ráfaga excesivo (Be)**: tamaño en exceso de la ráfaga de la red que intentará transmitir, además del valor B_c acordado durante el *T* predefinido.

Estos parámetros son unidireccionales, de modo que un circuito virtual puede asegurar diferentes valores de $CIR/B_c/B_e$ para cada dirección.

Si se aceptan los valores proporcionados, se definirá *T* por medio de la fórmula siguiente:

$$T = B_c/CIR \qquad (21.1)$$

También es posible especificar los valores de *CIR* y *T*, en cuyo caso el valor de la ráfaga de tráfico B_c se convertirá en el parámetro derivado. Como regla, para controlar ráfagas de tráfico, el intervalo *T* se elige de 1-2 segundos cuando se transmiten datos y dentro del intervalo de varias decenas o cientos de milisegundos cuando se transmite voz.

La figura 21.6 muestra la relación entre *CIR*, B_c, B_e y *T* (*R* es la velocidad del enlace de acceso; f_1 a f_5 son las tramas).

El parámetro principal con base en el que el suscriptor y el proveedor de servicio de red tienen un acuerdo cuando se establece una conexión virtual es el CIR. Para PVC, este acuerdo forma parte del contrato para proporcionar servicios de red. Cuando se establecen SVC, el acuerdo se hace automáticamente por medio del protocolo Q.933, mientras que los parámetros de conexión requeridos (*CIR*, B_c y B_e) se transmiten en el paquete de solicitud de conexión.

Dado que la velocidad de datos se mide durante un intervalo específico, *T* sirve como intervalo de medición durante el cual se verifican las condiciones del acuerdo. En general,

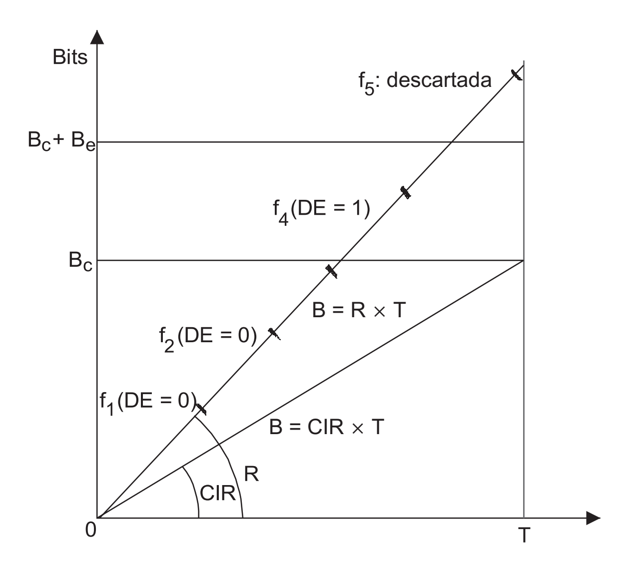


FIGURA 21.6 Reacción de la red al comportamiento del usuario.

durante este intervalo, el usuario no debe transmitir datos hacia la red a la velocidad promedio que excede CIR. Si el usuario violó este acuerdo, la red no garantizará la entrega de tales tramas y las marcará con el atributo de **descartar elegibilidad (DE, Discard Elegibility)** establecido a 1. Esto significa que tales tramas son las primeras candidatas para descartar. Las tramas con este atributo habilitado se retrasarán desde la red solamente si los switches de red están sobrecargados. La red no se encuentra congestionada y las tramas con el atributo DE = 1 se entregan al destino.

Tal comportamiento tolerante de la red corresponde al caso en el que el volumen total de los datos transmitidos por el usuario durante todo el periodo T no exceda $B_c + B_e$. Si se ha seguido este umbral, la trama se descartará inmediatamente sin establecer el atributo DE.

La figura 21.6 ilustra un caso en el cual cinco tramas se transmitieron hacia la red durante T. La tasa o velocidad promedio de datos en este intervalo fue de R bps y excede el valor CIR. Las tramas f_1, f_2 y f_3 se entregaron en la red de modo que la cantidad de datos no excede el umbral B_c; por lo tanto, se transmitieron adicionalmente con el atributo DE = 0. Los datos de f_4, agregados a los de f_1, f_2 y f_3, excedieron el valor B_c pero aún no el umbral $B_c + B_e$. Por consiguiente, también se transmitió f_4 adicionalmente; sin embargo, se estableció el atributo DE = 1. Los datos de f_5, al ser agregados a los datos de las tramas transmitidas con anterioridad, excedieron el umbral $B_c + B_e$; debido a esto, se descartó f_5.

Para controlar los parámetros de acuerdo, todos los switches Frame Relay soportan el algoritmo de cubeta con fuga. Este algoritmo pertenece a la misma clase de algoritmos que la del algoritmo de cubeta de estafeta estudiado en el capítulo 20. También permite controlar la velocidad promedio y las ráfagas de tráfico, pero hace esto de una manera ligeramente distinta.

El algoritmo de cubeta con fuga utiliza el contador C para contar bytes recibidos del usuario. Cada T segundos, este contador se disminuye por el valor B_c (o se restablecerá a 0 si el valor del contador es menor que B_c). Todas las tramas cuyos datos no incrementan el valor del contador de modo que excederían el umbral B_c se pasan a la red con el atributo DE = 0. Las tramas cuyos datos incrementaron el valor del contador arriba de B_c pero no provocaron que excediera el umbral $B_c + B_e$ también se pasan a la red; no obstante, esta vez el atributo DE se establece a 1. Finalmente, el switch descarta las tramas cuyos datos llevan el valor del contador por arriba de $B_c + B_e$.

El usuario también puede crear un acuerdo con el proveedor de servicio según el cual no todos sino únicamente parte de los parámetros QoS se tienen en cuenta para un circuito virtual específico.

Por ejemplo, es posible utilizar sólo parámetros CIR y B_c. Esta variante asegura una superior calidad de servicio, pues las tramas del usuario nunca son descartadas de inmediato por el switch, sino que éste únicamente marca las tramas que excedan el umbral B_c durante T por el atributo DE = 1. Si la red no está congestionada, las tramas de un circuito virtual de esta naturaleza siempre se entregan hacia el nuevo destino, incluso si el usuario violó constantemente su acuerdo con la red.

Existe otra solicitud conocida para QoS: aquella cuando sólo el umbral B_e está sujeto al acuerdo y se considera $CIR = 0$. Todas las tramas de un circuito de esta clase se marcan de inmediato mediante el atributo DE = 1. Sin embargo, se envían a la red y se descartarán únicamente si se excede el umbral B_e. El periodo de verificación T en este caso se calcula como B_e/R, donde R es la velocidad de acceso del enlace.

Como se aprecia en esta descripción, el algoritmo de cubeta con fuga controla las ráfagas de tráfico de manera más estricta que el de cubeta de estafeta. Este último algoritmo permite al tráfico acumular el tamaño de ráfaga durante periodos de baja actividad de la red y posteriormente utilizar las reservas acumuladas durante los periodos de ráfagas. El algoritmo

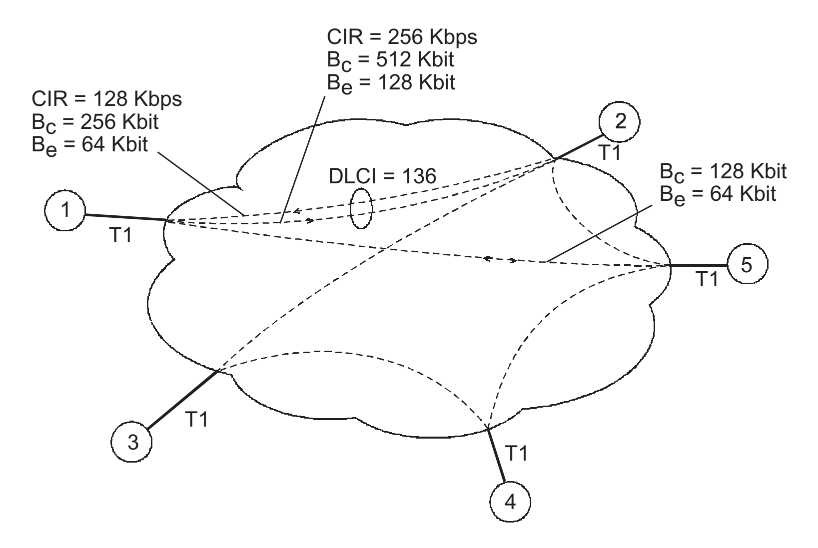


FIGURA 21.7 Uso de una red Frame Relay.

de cubeta con fuga no proporciona esta posibilidad, pues *C* se restablece a la fuerza a cero a medida que expira toda *T*, independientemente del número de bytes recibidos del usuario durante este periodo.

La figura 21.7 muestra el ejemplo de la red Frame Relay con cinco departamentos remotos. Por lo regular, el acceso a la red está asegurado mediante los enlaces con el ancho de banda que excede el valor *CIR*. Sin embargo, en este caso, el usuario paga por los valores solicitados de *CIR*, B_c y B_e, no por el ancho de banda del enlace. Por ejemplo, si se utiliza una línea T1 como un enlace de acceso y el usuario ha solicitado servicio para *CIR* = 128 Kbps, pagará únicamente por la velocidad de datos de 128 Kbps. La velocidad de datos del enlace T1, que es de 1544 Mbps, influirá sólo en el límite superior de la ráfaga posible: $B_c + B_e$.

Los parámetros de QoS pueden ser diferentes para direcciones distintas del circuito virtual. Por ejemplo, en la figura 21.7, el suscriptor 1 se encuentra conectado al suscriptor 2 mediante el circuito virtual DLCI = 136. En la dirección del suscriptor 1 al suscriptor 2, el circuito tiene una velocidad de datos promedio de 128 Kbps con B_c = 256 kb (el intervalo *T* fue medido en segundos) y B_e = 64 kb. Cuando se transmiten los datos en la dirección inversa, la velocidad promedio de datos puede alcanzar el valor de 256 Kbps, con B_c = 512 kb y B_e = 128 kb.

El mecanismo de reservación de ancho de banda promedio y ráfaga máxima es el mecanismo principal para asegurar QoS en redes Frame Relay.

Los acuerdos deben concluirse de manera tal que se asegure que la suma de las velocidades promedios de datos de los circuitos virtuales no excedan las capacidades de los puertos del switch de la red. Cuando se solicitan circuitos permanentes, el administrador mantiene la responsabilidad principal para hacerlo; al establecer circuitos conmutados, esta responsabilidad se delega al software de conmutación. Cuando se especifican correctamente las obligaciones mutuas, la red hace su mejor esfuerzo para eliminar la congestión al descartar tramas que tienen el atributo DE = 1 y tramas que han excedido el umbral $B_c + B_e$.

La tecnología Frame Relay define un algoritmo de control de flujo opcional, el cual es un mecanismo de información a los usuarios finales acerca de la congestión en los switches de red (sobre flujo con tramas no procesadas). El tipo de notificación de congestión explícito hacia delante (FECN, por sus siglas para Forward Explicit Congestion Notification) informa acerca de esta condición. Con base en el valor de este bit, el receptor debe informar al transmisor (utilizando protocolos de capa superior como TCP/IP, SPX, etc.) que ha de reducir la intensidad de la transmisión de tramas en la red.

El bit de notificación de congestión explícito de retroceso (BECN, por Backward Explicit Congestion Notification) informa al transmisor respecto a la congestión de la red, lo cual requiere que el transmisor reduzca de inmediato la velocidad de transmisión. Por lo regular, el bit BECN es procesado al nivel de los dispositivos de acceso de la red Frame Relay: múltiples torres y dispositivos CSU/DSU. El protocolo Frame Relay no requiere dispositivos que reciban tramas con bits FECN y BECN establecidos para detener inmediatamente la transmisión de tramas, como era el caso con las redes X.25. Estos bits sirven como indicaciones para protocolos de capa superior (TCP, SPX, FTP, etc.) con el fin de reducir la velocidad de transmisión de paquetes. Como el control de flujo por el receptor y el transmisor se lleva a cabo de manera diferente en protocolos distintos, los diseñadores de Frame Relay han tomado en cuenta ambas direcciones de transmisión de información de control acerca de la congestión de la red.

21.5 TECNOLOGÍA ATM

PALABRAS CLAVE: ATM, ISDN de banda ancha (B-ISDN, Broadband-ISDN), PDH, SDH/SONET, IP, SNA, Ethernet, PNNI, soporte de QoS, cinco clases de tráfico: A, B, C, D y X, tasa o velocidad constante de bits (CBR, Constant Bit Rate), tasa o velocidad variable de bits (VBR, Variable Bit Rate), retardo de empaquetamiento, velocidad pico de celdas (PCR, Peak Cell Rate), velocidad sostenida de celdas (SCR, Sustained Cell Rate), velocidad mínima de celdas (MCR, Minimum Cell Rate), tamaño máximo de ráfaga (MBS, Maximum Burst Size), relación de celdas perdidas (CLR, Cell Loss Ratio), retardo de transferencia de celdas (CTD, Cell Transfer Delay), variación del retardo de celda (CDV, Cell Delay Variation), tasa de bits no especificada (UBR, Unspecified Bit Rate), administración de recursos especial (RM, Resource Management), celdas de administración de recursos hacia delante (FRM, Forward Resource Management), celdas de administración de recursos hacia atrás (BRM, Backward Resource Management) y ciclos o loops de retroalimentación.

La tecnología ATM se diseñó como un transporte universal para una nueva generación de redes con servicios integrados conocidas como **ISDN de banda ancha** (B-ISDN, por sus siglas en inglés). Principalmente, ATM fue el segundo intento de construir una red convergente después del fracaso de ISDN para obtener este objetivo. En contraste con Frame Relay, que al inicio estaba destinado sólo para transmitir tráfico computacional elástico, las intenciones de los diseñadores de ATM fueron mucho más extensas y ambiciosas.

De acuerdo con los planes de los diseñadores, ATM debía asegurar varias de las capacidades siguientes:

- El sistema de transporte simple para transmitir simultáneamente tráfico computacional y multimedia (voz y videos), el cual es muy sensible a los retardos; la QoS para cada clase de tráfico debe corresponder a sus requerimientos.

- La jerarquía de las velocidades de transmisión que abarcan desde las decenas de Megabits por segundo hasta varios gigabits por segundo, con un ancho de banda garantizado para aplicaciones críticas.
- La posibilidad de utilizar la infraestructura existente de enlaces físicos o protocolos físicos: PDH, SDH o LAN de alta velocidad.
- La interacción con los protocolos existentes de LAN y WAN, como IP, SNA, Ethernet e ISDN.

Es necesario señalar que la mayoría de estos objetivos se lograron con éxito. A partir de mediados de la década de 1990, ATM ha sido una tecnología de trabajo que asegura el soporte más completo y consistente de parámetros de QoS para usuarios de red. Además, ATM, como cualquier otra tecnología de circuitos virtuales, proporciona amplias capacidades en el campo de la resolución de problemas de ingeniería de tráfico.

El desarrollo de los estándares ATM (RFC 2514, RFC 2515, RFC 2761, RFC 3116, etc.) lo realizaron muchos fabricantes de equipo de telecomunicaciones y portadores de comunicaciones participantes en el fórum ATM. Los comités especiales de ITU-U y ANSI también intervinieron en este trabajo.

A pesar del éxito evidente de la tecnología ATM, que funciona en los troncales de los portadores de comunicaciones más grandes, ha demostrado tener limitaciones. De este modo, ATM no ha dejado fuera de uso las otras tecnologías ni se convertirá en la única tecnología de transporte de las redes de telecomunicaciones, aun cuando esto parecía inevitable a mediados de la década de 1990 debido a las ventajas tecnológicas obvias de ATM. En teoría, los protocolos de capa de aplicación pueden utilizar directamente ATM de manera que la red pueda funcionar sin IP ni TCP/UDP. ATM proporciona muchas características requeridas para obtener su objetivo, incluidos el soporte para toda clase de tráfico, la escalabilidad y un protocolo de enrutamiento nativo complejo. Sin embargo, esto será posible sólo si la red es tecnológicamente homogénea. Para este propósito, todas las redes de todos los proveedores de servicio deben soportar ATM. Como se observa con facilidad, un enfoque así contradice el principio fundamental del trabajo en interredes, de acuerdo con el cual cada red puede soportar su propia tecnología de transporte y la capa de red combina estas redes constituyentes en la interred unificada.

Por lo tanto, IP tomó la posición dominante en la capa de red a mediados de la década de 1990 y aún se usa para el trabajo en interredes. En cuanto a ATM, llegó a ser una de las tecnologías con base en la cual funcionan muchas redes constituyentes.

21.5.1 Principios fundamentales de la operación de ATM

La red ATM tiene la estructura clásica de una WAN de gran escala. Las estaciones de trabajo (nodos terminales) están conectadas a los switches de capa inferior en los que se utilizan enlaces individuales; a su vez, estos switches se conectan a switches de capa superior. Los switches ATM usan direcciones de nodos terminales de 20 bytes para ruteo de tráfico según la técnica de circuito virtual. Para redes privadas ATM, se define el protocolo de enrutamiento NNI privado (PNNI, por sus siglas en inglés), mediante el cual los ruteadores pueden construir de forma automática tablas de ruteo y en relación con los requerimientos de ingeniería de tráfico. Como regla, las direcciones de acuerdo con el estándar E.164 se utilizan en redes ATM públicas, lo cual simplifica la interconexión de estas redes a las redes telefónicas. Las direcciones ATM tienen una estructura jerárquica similar a los números telefónicos o direcciones IP. Esto asegura la escalabilidad ATM a cualquier nivel requerido, incluso a la red mundial.

Para acelerar la conmutación en redes a gran escala, se emplea el concepto de una *trayectoria virtual*, que conecta circuitos virtuales con una ruta común en la red ATM que une el nodo de origen y el nodo terminal, o alguna parte en común de la ruta entre dos switches de red. Esta propiedad también mejora la escalabilidad de ATM, pues reduce de modo considerable las conexiones virtuales soportadas por el ruteador troncal, con lo que mejora la eficacia de su operación.

El estándar ATM no introduce especificaciones individuales para implementación de capa física. A este respecto, se basa en la tecnología SDH/SONET y adopta jerarquía de velocidad. De acuerdo con ello, la velocidad de acceso de inicio proporcionada a los usuarios de la red es la velocidad de acceso STM-1, que alcanza 155 Mbps. El equipo troncal de ATM funciona a velocidades superiores: STM-4 a 622 Mbps y STM-16 a 2.5 Gbps. También existe equipo ATM que soporta velocidades PDH, como 34 Mbps y 45 Mbps.

Todas las características mencionadas respecto a la tecnología ATM no sirven como evidencia de que sea ésta una tecnología "específica"; más bien, es una tecnología WAN típica basada en la técnica de circuito virtual. Las características específicas de la tecnología ATM residen en el servicio de calidad de varias clases de tráfico.

La propiedad más importante de ATM que la separa de otras tecnologías es *el soporte de QoS integrado para todas las clases de tráfico.*

Para asegurar esta propiedad, los diseñadores de ATM analizaron cuidadosamente todos los tipos de tráfico y llevaron a cabo su clasificación. El lector conoció esta clasificación en el *capítulo 7* cuando se consideraron los requerimientos de QoS de diferentes aplicaciones. Recuérdese que la clasificación ATM divide todo el tráfico en cinco clases: A, B, C, D y X. Las primeras cuatro clases representan el tráfico de aplicaciones típicas, las cuales tienen un conjunto estable de requerimientos para pérdidas y retardos de paquetes. Otra característica distintiva de vitales aplicaciones es que generan tráfico caracterizado por una velocidad constante de bits (CBR, por sus siglas en inglés) o una velocidad variable de bits (VBR, por sus siglas en inglés). La clase X está reservada para aplicaciones únicas para las cuales el conjunto de características y requerimientos QoS no puede clasificarse como perteneciente a una de las primeras cuatro clases.

Sin embargo, el número de clases de tráfico en cualquier clasificación no incluye algún cambio principal en la solución de este problema: encontrar una forma de soportar con éxito clases de tráfico elásticas y sensibles al retardo en el mismo canal. Los requerimientos de estas clases son casi siempre mutuamente contradictorios. Una contradicción de esta clase es el requerimiento para el tamaño de la trama.

El tráfico elástico se beneficia del incremento en el tamaño de la trama, pues esto reduce el gasto para la información de control. En el ejemplo de la trama Ethernet, se observó que la velocidad efectiva de datos puede cambiar a más del doble cuando se modifica el tamaño del campo de datos de su valor mínimo de 46 bytes hasta el valor máximo de 1 500 bytes. Desde luego, el tamaño de la trama no puede ser incrementado infinitamente porque en este caso la idea de conmutación de paquetes perdería su sentido. No obstante, para el tráfico elástico en un nivel de velocidades contemporáneo, es aceptable un tamaño de trama de millares de bytes.

Por el contrario, el tráfico sensible al retardo se sirve mejor cuando se utilizan tramas pequeñas de decenas de bytes. Cuando se emplean tramas grandes, comienzan a ser notorios dos efectos indeseables:

- Retardos largos de tramas de baja prioridad en las colas.
- Retardo de empaquetamiento.

Considérense estos efectos en el ejemplo del tráfico de voz.

Sabemos que el *tiempo de espera en colas* podrá reducirse si las tramas del tráfico sensible al retardo se sirven en la cola de prioridad. Sin embargo, si el tamaño del paquete puede variar en un amplio intervalo (por ejemplo, desde 29 hasta 4 500 bytes, como ocurre en la tecnología FDDI), aun cuando a los paquetes de voz se les asigne la prioridad más alta para servicio en los switches, el tiempo de espera para paquetes computacionales podrá resultar demasiado largo para ser aceptable. Por ejemplo, un paquete de 4 500 bytes se transmitirá al puerto de salida a la velocidad de 2 Mbps (la velocidad típica de operación del puerto de acceso Frame Relay) en 18 milisegundos. Cuando se combina tráfico, es necesario transmitir 144 muestras de voz a través del mismo puerto durante el mismo tiempo. No es deseable interrumpir la transmisión del paquete, pues en una red distribuida el gasto para informar al switch vecino acerca de esta interrupción y la continuación subsiguiente de la transmisión ha demostrado ser demasiado alto.

El **retardo de empaquetamiento** es el tiempo durante el cual la primera muestra de voz espera que el paquete sea completamente formado y enviado en la red. El mecanismo de este retardo se ilustra en la figura 21.8.

El códec produce muestras de voz de manera periódica al mismo intervalo. Por ejemplo, el códec PCM mostrado en la ilustración realiza esto a una frecuencia de 8 kHz, es decir, cada 125 μs (microsegundos). Si el lector utiliza tramas Ethernet del tamaño máximo para transmisión de voz, cada trama conducirá 1500 muestras de voz, pues cada muestra está codificada por 1 byte de datos. Como resultado, la primera muestra colocada en la trama Ethernet tendrá que esperar a que se envíe la trama en la red durante un tiempo de $(1\,500 - 1) \times 125 = 187\,375$ μs, o aproximadamente 187 ms (milisegundos). Este retardo es bastante significativo para el tráfico de voz. Por ejemplo, de acuerdo con las recomendaciones ITU-T, este retardo no debe exceder los 150 ms. Es importante observar que el retardo de la trama no depende de la tasa o velocidad de bits del protocolo. Por el contrario, sólo depende de la frecuencia de operación del códec y del tamaño del campo de datos de la trama. Esto lo separa el retardo de la cola, el cual se reduce con el incremento de la velocidad de bits.

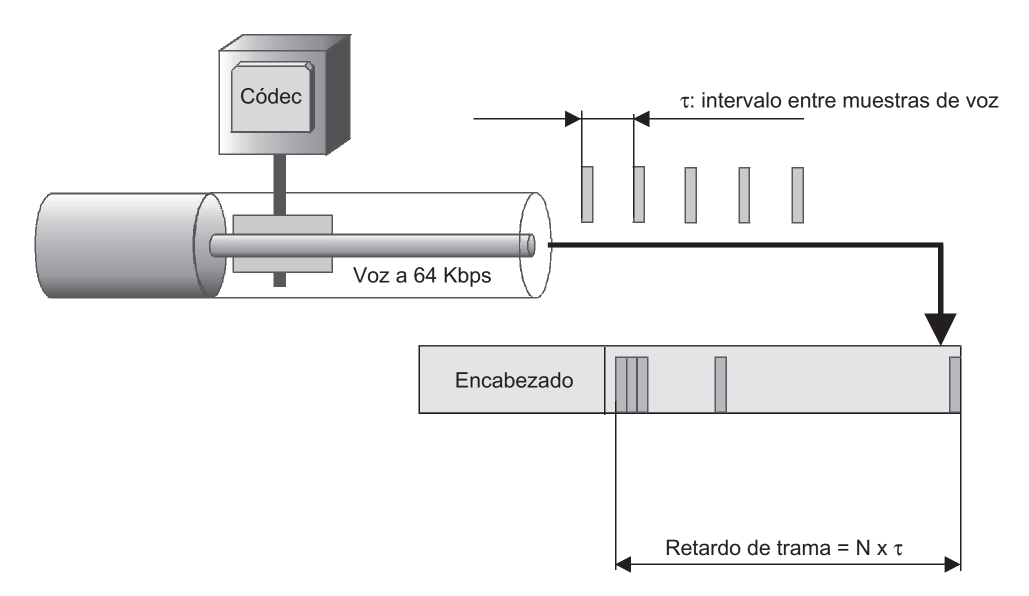


FIGURA 21.8 Retardo de empaquetamiento.

El tamaño de la trama ATM con el tamaño del campo de datos de 48 bytes es un compromiso entre los requerimientos del tráfico elástico y el sensible al retardo. En otras palabras, es posible establecer que este compromiso lo consiguieron especialistas en telefonía y computación: los primeros insistían en un tamaño del campo de datos de 32 bytes, mientras que los segundos querían 64 bytes. Debido a este tamaño pequeño y fijo de la trama ATM, ha llegado a ser conocida como **celda**.

Con una longitud del campo de datos de 48 bytes, una celda ATM simple suele conducir 48 muestras de voz tomadas con un intervalo de 125 μs. Por lo tanto, la primera muestra debe esperar aproximadamente 6 ms antes de que la celda sea enviada en la red. Ésta es la principal razón por la que los especialistas en telefonía insistían en reducir el tamaño de la celda. Los 6 milisegundos están cerca del umbral después del cual la calidad de transmisión de voz comienza a degradarse. Si se elige el tamaño de la celda común de 32 bytes, el retardo del empaquetamiento sería de 4 ms, lo que garantizaría la transmisión de voz de calidad superior. La razón por la que los especialistas computacionales se esfuerzan para incrementar el campo de datos a 64 bytes también está justificada, pues si se satisface esta condición, aumentaría la velocidad de datos efectiva. La redundancia de los datos de servicio cuando se utiliza un campo de datos de 48 bytes es de 10%; cuando se emplea un campo de datos de 32 bytes, se incrementa a 16 por ciento.

Para el paquete que abarca 53 bytes, a la velocidad de 155 Mbps, el tiempo de transmisión de la trama hacia el puerto de salida es menor de 3 μs. De este modo, dicho retardo no es demasiado significativo para el tráfico cuyos paquetes deben transmitirse cada 125 μs.

Para asegurar que los paquetes contienen la dirección del nodo de destino y garantizar que el porcentaje de la información de control no exceda el tamaño del campo de datos del paquete, la tecnología ATM pone en práctica una técnica que es estándar para las WAN: la transmisión de celdas de acuerdo con la técnica del circuito virtual. La longitud total del número de circuito virtual es de 24 bits, suficiente para dar servicio a un gran número de conexiones virtuales por cada puerto del switch de la WAN a gran escala (posiblemente, a escala mundial) basada en ATM.

Es necesario señalar que utilizar celdas pequeñas en ATM proporciona conexiones excelentes para un servicio de alta calidad para el tráfico sensible al retardo. El precio por esta perfección es la elevada carga sobre los switches ATM cuando funcionan a velocidades altas. Recuérdese que la cantidad de trabajo llevada a cabo por ruteador basado en cualquier tecnología es directamente proporcional al número de paquetes o tramas procesadas por unidad de tiempo. Desde luego, el uso de celdas con un tamaño del campo de datos de 48 bytes produce una carga muy alta sobre el switch ATM en comparación con, por ejemplo, un switch Ethernet que funciona con tramas de 1500 bytes. Debido a esto, los switches ATM no podrían exceder el límite de velocidad de interfase de 622 Mbps durante largo tiempo. Sólo recientemente comenzaron a soportar velocidades de 2.5 Gbps.

La selección de una celda de datos pequeña de tamaño fijo no resuelve por sí misma el problema de combinar diferentes clases de tráfico en la misma red; más bien, sólo asegura los requisitos previos para encontrar una solución a él. *Con el fin de resolver por completo esta tarea, la tecnología ATM implementa y desarrolla las ideas de proporcionar el ancho de banda y la QoS bajo demanda ("on demand"), una idea implementada en la tecnología Frame Relay*.

En la tecnología ATM, para cada clase de tráfico existe un conjunto de parámetros cuantitativos que deben ser especificados por la aplicación. Para el tráfico clase A, es necesario especificar una velocidad constante a la cual la aplicación enviará sus datos en la red, mientras que para el tráfico clase B, se debe especificar la máxima velocidad posible, la velocidad promedio y la máxima ráfaga posible. Para el tráfico de voz, es posible no sólo especificar la importancia de la sincronización entre el transmisor y el receptor, sino también propor-

cionar características cuantitativas con las que se señalen umbrales superiores para retardo y variación de retardo.

ATM soporta el siguiente conjunto de parámetros cuantitativos principales para el tráfico de circuito virtual:

- **Tasa o velocidad pico de la celda (PCR, Peak Cell Rate):** velocidad pico de transmisión de datos.
- **Tasa o velocidad sostenida de la celda (SCR, Sustained Cell Rate)**: velocidad promedio de transmisión de datos.
- **Tasa o velocidad mínima de la celda ((MCR, Minimum Cell Rate)**: velocidad mínima de transmisión de datos.
- **Tamaño máximo de la ráfaga (MBS, Maximum Burst Size)**: tamaño máximo de la ráfaga de datos.
- **Relación de pérdida de celdas (CLR, Cell Loss Ratio)**: porción de celdas perdidas.
- **Retardo de transferencia de celdas (CTD, Cell Transfer Delay)**: retardo de transmisión de celdas.
- **Variación del retardo de celdas (CDV, Cell Delay Variation)**: variación del retardo de transmisión de celdas.

Los parámetros de velocidad se miden en celdas por segundo, MBS se mide en celdas y los parámetros temporales se miden en segundos. MBS especifica el número de celdas que la aplicación puede transmitir a la PCR, a condición de que se especifique la velocidad promedio. La porción de celdas perdidas es el promedio que existe entre el número de celdas perdidas y el número número total de celdas enviadas a través de esta conexión virtual. Como las conexiones virtuales son dúplex, es posible especificar valores individuales para cada dirección de la transmisión de datos.

La tecnología ATM utiliza un enfoque no provisional para la interpretación del término QoS. Por lo regular, QoS se caracteriza por los parámetros de ancho de banda (en este caso son RCR, SCR, MCR y MBS), los parámetros de retardo de paquete (CTD y CDV) y los parámetros de confiabilidad de transmisión de paquetes (CLR). En ATM, las características de velocidad de información se denominan parámetros de tráfico. No están incluidos en el número de parámetros de QoS aunque principalmente son tales parámetros. En ATM, los parámetros de QoS incluyen únicamente CTD, CDV y CLR. La red intenta asegurar un nivel de servicio que soporte los valores requeridos para los parámetros de tráfico, para retardos de celda y para el porcentaje de celdas perdidas.

El acuerdo entre la aplicación y la red ATM se conoce como *contrato de tráfico.* Su principal diferencia con los acuerdos utilizados en redes Frame Relay es la selección de una de las varias clases de tráfico para la cual, aparte de los parámetros de ancho de banda, es posible especificar los parámetros de retardo de celda y el parámetro de confiabilidad de entrega de celda. En Frame Relay, sólo existe una clase de tráfico y está caracterizada únicamente por parámetros de ancho de banda.

Si el soporte de los parámetros de ancho de banda y los parámetros de QoS no es crítico para la aplicación, podrá omitirlos y especificar el atributo de "mejor esfuerzo" en la solicitud para establecer una conexión. Este tipo de tráfico se conoce como tráfico de **tasa de bits no especificada** (UBR, Unspecified Bit Rate).

Después de concluir el contrato de tráfico que relaciona a la conexión virtual específica, la red ATM proporciona varios protocolos y servicios necesarios para asegurar la QoS solicitada. Para el tráfico UBR, la red asigna recursos como sea posible (es decir, los recursos actualmente disponibles para asignación) puesto que no están siendo usados por conexiones virtuales que hayan solicitado parámetros de QoS específicos.

Capas superiores de la red

<table>
<tr><td rowspan="3">Capas de adaptación ATM ATM (AAL1-5)</td><td rowspan="2">Subcapa de convergencia (CS)</td><td>Parte común de la subcapa de convergencia</td></tr>
<tr><td>Parte de servicio específico de la subcapa de convergencia</td></tr>
<tr><td colspan="2">Subcapa de segmentación y reensamblado (SAR)</td></tr>
<tr><td colspan="3">Capa ATM (ruteo de paquetes, multiplexado, control de flujo, manejo de prioridad)</td></tr>
<tr><td rowspan="2">Capa física</td><td colspan="2">Subcapa de reconciliación de transmisión</td></tr>
<tr><td colspan="2">Subcapa dependiente del medio</td></tr>
</table>

FIGURA 21.9 Estructura de la pila de protocolos ATM.

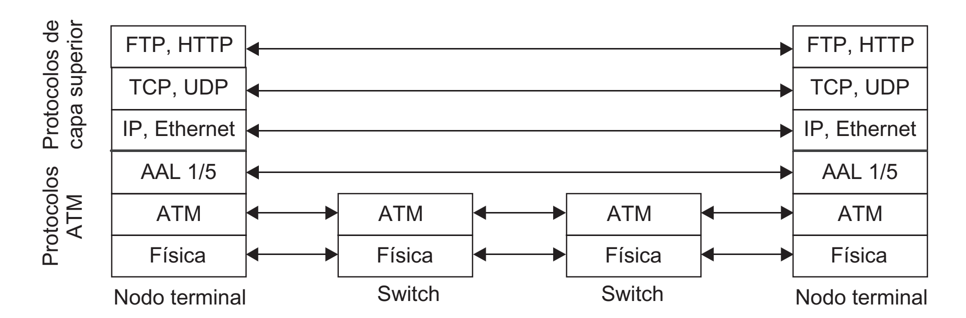


FIGURA 21.10 Distribución de protocolos ATM sobre switches y nodos terminales.

21.5.2 Pila de protocolo de ATM

La pila de protocolo de ATM se muestra en la figura 21.9 y la distribución del protocolo sobre nodos terminales y switches ATM se encuentra en la figura 21.10.

La pila de protocolo de ATM corresponde a las capas inferiores del modelo ISO/OSI e incluye la capa de adaptación de ATM (AAL, ATM Adaptation Layer), la capa ATM y la capa física. No hay correspondencia directa entre ATM y las capas del protocolo OSI.

21.5.3 Capa de adaptación de ATM

La AAL es el conjunto de protocolos AAL1-AAL5 que convierten los mensajes de protocolos de capa superior de la red ATM en celdas ATM del formato requerido. Las funciones de estas capas corresponden convencionalmente a la capa de transporte OSI (como TCP y UDP). Los protocolos AAL funcionan solamente en nodos terminales de la red, como los protocolos de transporte de la mayoría de las tecnologías de red.

Cada protocolo de la capa AAL procesa tráfico del usuario de una clase específica. En las etapas iniciales de la estandarización, cada clase de tráfico tenía su correspondiente protocolo AAL, del cual recibía los paquetes desde el protocolo de capa superior en el nodo terminal y utilizaba el protocolo apropiado para solicitar los parámetros de tráfico y QoS para la conexión virtual específica requerida por la aplicación. En el transcurso de la evolución de los estándares ATM, esta correspondencia no ambigua entre las clases de tráfico

y los protocolos AAL ha desaparecido. Ahora es posible utilizar diferentes protocolos AAL para la misma clase de tráfico.

El AAL abarca dos subcapas.

- La subcapa inferior es la **capa de segmentación y reensamblado (SAR, Segmentation And Reassembly)**. Esta parte no depende del tipo de protocolo AAL (o, en consecuencia, de la clase de tráfico transmitido), pero segmenta el mensaje recibido por AAL desde el protocolo de capa superior. Después de crear la celdas ATM, SAR les proporciona encabezados apropiados y las pasa a la capa ATM para transmitirlas en la red.
- La subcapa superior de AAL es la **subcapa de convergencia (CS, Convergence Sublayer)**. Esta subcapa depende de la clase de tráfico que se transmite. El protocolo CS resuelve problemas tales como el de asegurar la sincronización entre los nodos transmisores y receptores (para el tráfico que requiere tal sincronización), control y recuperación de errores de bit en datos del usuario y el control de integridad del paquete del protocolo computacional que se transmite (X.25 o Frame Relay).

Para llevar a cabo sus tareas, los protocolos AAL utilizan información de control localizada en los encabezados AAL. Una vez que ha recibido las celdas que llegan a través del circuito virtual, SAR ensambla el mensaje fuente o de origen (generalmente dividido en varias celdas ATM) mediante el uso de encabezados AAL. Estos encabezados son invisibles para los switches ATM debido a que residen en el campo de datos de 48 bits de la celda, lo que es normal para un protocolo de capa superior. Una vez que ha ensamblado el mensaje de origen, AAL verifica los campos de control del encabezado y portador de la trama AAL y, con base en esta verificación, decide si la información recibida es correcta.

Cuando se transmite en los datos del usuario, el protocolo AAL no recupera datos perdidos ni corrompidos. Lo más que el protocolo AAL puede hacer es informar al nodo terminal acerca de un evento de esa naturaleza. Esto se hizo para acelerar la operación de los switches ATM en espera de que la pérdida y corrupción de datos sean eventos poco frecuentes. La recuperación de datos perdidos (o ignorar un evento así) es una tarea delegada a protocolos de capa superior que no se incluyen en la pila del protocolo ATM.

El protocolo **AAL1** suele servir al tráfico de clase A con CBR, lo cual es crítico, por ejemplo, para voz o vídeo digital y es sensible a los retardos. Las redes ATM transmiten ese tráfico de manera tal que simula enlaces digitales rentados normales. El encabezado AAL1 ocupa 1 o 2 bytes en el campo de datos de la celda ATM y deja 47 o 46 bytes para los datos del usuario, respectivamente. Un byte del encabezado está asignado para la numeración de la celda de modo que el nodo receptor pueda decidir si ha recibido o no todas las celdas enviadas a él. Cuando se envía tráfico de voz, se conoce la huella temporal de cada muestra, pues se siguen uno a otro a intervalos de 125 µs. Así, si se pierde la celda, se podrá corregir la temporización de la siguiente celda sólo con desplazarla 125 x 46 µs. La pérdida de varios bytes de una muestra de voz no es crítica, porque en el nodo receptor el equipo suaviza la señal. Las tareas del protocolo AAL1 incluyen suavizar la irregularidad de la llegada de las celdas al nodo de destino.

El protocolo **AAL2** fue diseñado para transmitir tráfico de clase B; posteriormente, se excluyó de la pila del protocolo ATM. En la actualidad, el tráfico de clase B se transmite mediante el uso del protocolo AAL1, AAL3/4 o AAL5.

El protocolo **AAL3/4** procesa tráfico de ráfagas típico para LAN. Ésta es una VBR, y el tráfico se procesa de tal modo que se eviten pérdidas de celdas; sin embargo, el switch

puede retardar las celdas. El protocolo AAL3/4 lleva a cabo un complicado procedimiento de control de errores cuando se transmiten las celdas. Para conseguir esto, numera cada parte del mensaje de origen y cada celda le suministra la suma de verificación. No obstante, si las celdas llegan a perderse o corromperse, esta capa no intentará recuperarlas; en su lugar, descartará todo el mensaje, es decir, todas las celdas restantes. Esto se debe a que para el tráfico computacional o la voz comprimida, la pérdida de incluso una sola celda es un error fatal. El protocolo AAL3/4 es el resultado de mezclar los protocolos AAL3 y AAL4, lo cual aseguró el soporte para el tráfico computacional en el que se utilizan protocolos orientados a conexión y sin conexión, respectivamente. Sin embargo, debido a que usaban formatos de encabezado cerrado y una lógica de operación semejante, se combinaron los protocolos AAL3 y AAL4.

El protocolo **AAL5** es una versión simplificada del protocolo AAL4; funciona más rápido debido a que no calcula la suma de verificación para cada celda del mensaje; por el contrario, calcula la suma verificadora para todo el mensaje de origen y la coloca en la última celda del mensaje. Inicialmente, el protocolo AAL5 fue diseñado para transmitir las tramas de redes Frame Relay. Sin embargo, hoy en día se utiliza para transmitir cualquier tráfico computacional (RFC 2684). AAL5 puede soportar diferentes parámetros de QoS, excepto aquellos que se relacionan con la sincronización entre el transmisor y el receptor. Por lo tanto, normalmente se emplea para soportar toda clase de tráfico vinculado con la transmisión de datos computacionales (es decir, el tráfico de las clases C y D). Algunos fabricantes de equipo usan AAL5 para dar servicio al tráfico CBR; delegan la tarea de la sincronización a los protocolos de capa superior. AAL5 funciona no sólo en nodos terminales sino también en switches ATM; empero, en los switches lleva a cabo funciones de control que no están relacionadas con la transmisión de los datos del usuario. En switches, AAL5 soporta protocolos de servicio de capa superior involucrados en establecer conexiones virtuales.

Existe una interfase especial entre la capa AAL y la aplicación que necesita transmitir tráfico utilizando la red ATM. Al usar esta interfase, la aplicación (por ejemplo, un protocolo de redes de computadoras o un módulo de muestreo de voz) solicita el servicio necesario mediante la determinación del tipo de tráfico y sus parámetros de QoS. La tecnología ATM permite dos variantes de definición de parámetros QoS: directamente por cada aplicación y al emplear los valores predeterminados según el tipo de tráfico. Este último método simplifica la tarea del diseñador de la aplicación, pues la selección del retardo máximo y la variación del retardo para la entrega de la celda se delegan al administrador de la red.

Los protocolos AAL son incapaces de asegurar por sí mismos el tráfico requerido en los parámetros QoS. Para observar las condiciones del contrato de tráfico, es necesario asegurar la operación coordinada de todos los switches de la red a lo largo del circuito virtual. Esta tarea la lleva a cabo el protocolo ATM que asegura la transmisión de las celdas de diferentes conexiones virtuales con el nivel requerido de QoS.

21.5.4 Protocolo ATM

El protocolo ATM toma aproximadamente la misma posición en la pila del protocolo ATM que la sostenida por IP en la pila TCP/IP o que la LAP-F en la pila del protocolo Frame Relay. El protocolo ATM transmite celdas y utiliza switches cuando el circuito virtual se ha establecido y configurado, lo cual significa que esta tarea se basa en las tablas de conmutación del puerto.

Para realizar la conmutación, el protocolo ATM usa el **número del circuito virtual**, que se divide en dos partes en la tecnología ATM:

- El **identificador de trayectoria virtual** (VPI, Virtual Path Identifier).
- El **identificador de canal virtual** (VCI, Virtual Channel Identifier).

Además de esta tarea principal, el protocolo ATM también realiza algunas funciones relacionadas con permitir al usuario de la red observar el contrato de tráfico, marcar las celdas que lo violen, descartar dichas celdas en caso de congestión de la red y controlar el flujo de celdas para mejorar el rendimiento de la red (naturalmente, si todos los circuitos virtuales observan las condiciones del contrato de tráfico).

El formato de celda ATM se muestra en la figura 21.11.

El campo de *control de flujo genérico* se utiliza más allá del curso de la interacción entre el nodo terminal y el primer switch de la red. Sus funciones exactas todavía no están definidas.

Los campos *VPI y VCI* ocupan 1 y 2 bytes, en consecuencia. Estos campos especifican el número de conexiones virtuales divididas en las partes más significativa (VPI) y menos significativa (VCI).

El campo del *identificador del tipo de pago* abarca 3 bytes y especifica el tipo de datos conducidos por la celda: datos del usuario o datos de control (por ejemplo, cuando se establece una conexión virtual). Además, un bit de este campo se utiliza para indicar congestión de la red. Dicho bit se denomina *identificador de direccionamiento de congestión explícito* (EFCI, por sus siglas en inglés), desempeña el mismo papel que el bit FECN en la tecnología Frame Relay y pasa información acerca de la congestión de la red en la dirección del flujo de datos.

La *prioridad a la pérdida de celdas (CLP, Cell Loss Priority)* en esta tecnología desempeña el mismo papel que el campo *DE* en la tecnología Frame Relay. Los switches ATM usan este campo para marcar las celdas que violan el acuerdo de los parámetros de QoS de la conexión. Tales celdas se descartarán si se presenta congestión de la red. De este modo, la celda con CLP = 0 es una alta prioridad para la red, mientras que las celdas con CLP = 1 tienen una baja prioridad.

El campo de *control de error del encabezado* (HEC, Header Error Control) contiene la suma de verificación calculada para el encabezado de la celda. Para calcular la suma verificadora, se usa el código de corrección de errores de Hamming. Por ende, no sólo permite

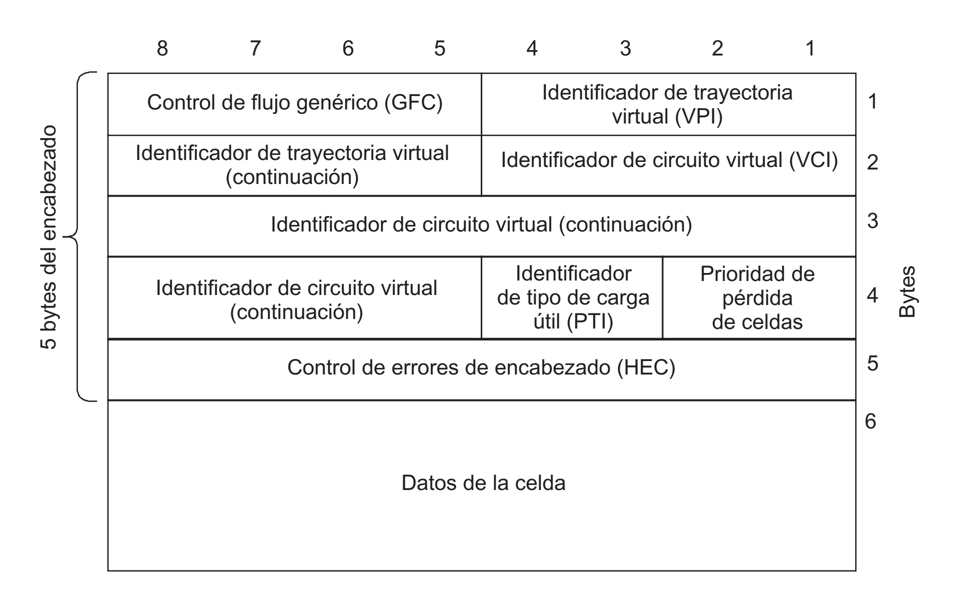


FIGURA 21.11 Formato de celda ATM.

detectar errores sino que también puede corregir todos los errores aislados (y, en condiciones favorables, incluso algunos errores duplicados). El campo *HEC* no sólo asegura la detección y corrección de errores en el encabezado, sino que al mismo tiempo facilita descubrir el límite de la trama en el flujo de bytes SDH, que es la capa física preferida para la tecnología ATM, o en el flujo de bits de la capa física basada en celdas. En ATM, no hay apuntadores que detectarían los límites de las celdas ATM en el campo de datos de la trama STS-n/STM-n de la tecnología SONET/SDH (semejantes a los apuntadores utilizados para determinar los límites de los contenedores virtuales de los canales T1/E1). Por lo tanto, el switch ATM calcula la suma de verificación para la secuencia de 5 bytes localizada en el campo de datos de la trama STM-n y, si la suma verificadora muestra que el encabezado de la celda ATM es correcto, el primer byte se convertirá en el límite de la celda. Si esto no es así, habrá un desplazamiento de un byte y continuará la operación. De este modo, la tecnología ATM detecta el flujo asincrónico de las celdas ATM en las tramas SDH sincrónicas o en el flujo de bits de capa física basado en celdas.

Los switches ATM podrán funcionar si se emplean dos modos:

- **Conmutación de trayectoria virtual.** En este modo, el switch direcciona la celda sólo con base en el campo *VPI* e ignora el valor VCI. Por lo regular, los switches troncales de redes regionales a gran escala funcionan de esta manera. Entregan las celdas de red en red solamente de acuerdo con la parte más significativa del número del circuito virtual, que corresponde a la idea de agregación de dirección. Como resultado, una trayectoria virtual corresponde al conjunto de circuitos virtuales agregados en el conjunto simple.
- **Conmutación de circuito virtual.** Después de entregar la celda a la red ATM local, los switches de esa red comienzan la conmutación de celdas, teniendo en cuenta tanto VPI como VCI. Sin embargo, para la conmutación necesitan sólo la parte menos significativa del número de conexión virtual; por ende, trabajan únicamente con VCI y dejan VPI sin cambio alguno.

Para crear un SVC, ATM utiliza protocolos que no se muestran en la figura 21.11. En este caso, el enfoque es similar al enfoque ISDN. Para establecer una conexión, se ha diseñado un protocolo por separado, **Q.2931**, el cual se puede clasificar condicionalmente como un protocolo de capa de red. Este protocolo tiene mucho en común con los protocolos Q.931 y Q.933 (incluido el número). Sin embargo, naturalmente, se introdujeron algunas modificaciones en el mismo relacionadas con el soporte de varias clases de tráfico y parámetros QoS adicionales. El protocolo Q.2931 depende de un protocolo más complejo de capa de enlace de datos denominado SSCOP, el cual asegura transmisión confiable de Q.2931 en sus tramas. A su vez, SSCOP funciona sobre el protocolo AAL5 requerido para dividir las tramas SSCOP en celdas ATM y ensambla estas celdas en tramas cuando entregan la trama SSCOP al switch de destino.

NOTA *Q.2931 apareció en la pila de protocolo ATM después de adoptarse la interfase UNI 3.1. En UNI 3.1, se utilizó en su lugar el protocolo Q.93B. Debido a la incompatibilidad entre Q.2931 y Q.93B, las versiones de la interfase UNI 3.0 y UNI 3.1 son también compatibles. La versión UNI 4.0 proporciona compatibilidad hacia atrás con UNI 3.1 porque está basada en los mismos protocolos de control que UNI 3.1.*

Las conexiones virtuales creadas con Q.2931 pueden ser de tipo símplex (unidireccional) o dúplex (bidireccional).

El protocolo Q.2931 también permite establecer conexiones virtuales punto a punto y punto a multipunto. El primer caso es soportado en todas las tecnologías basadas en circuitos

virtuales. El segundo caso es típico solamente para ATM y es el análogo de multicasting o multidirección, excepto con un nodo multidirigido simple. Cuando se establece una conexión de punto a multipunto, el nodo principal es el iniciador de esta conexión. En primer lugar, este nodo establece una conexión virtual con un nodo; luego, emplea una llamada especial para agregar nuevos miembros a esta conexión. El iniciador llega a ser la raíz del árbol de conexiones y los otros nodos participantes desempeñan la función de las "hojas". Los mensajes enviados por el nodo principal son recibidos por todas las hojas de conexión; sin embargo, los mensajes enviados por una hoja específica (en una conexión dúplex) solamente los recibe el nodo principal.

Los paquetes del protocolo Q.2931 destinados a establecer un SVC tienen los mismos nombres y los mismos propósitos de los paquetes del protocolo Q.933, los cuales se examinaron en este capítulo al describir la tecnología Frame Relay. Sin embargo, la estructura de sus campos es diferente.

La dirección del nodo terminal en los switches ATM es la dirección de 20 bytes.

Cuando operan en redes públicas, se emplea la dirección correspondiente al estándar E.164. Esta dirección tiene un formato flexible y puede dividirse en partes para asegurar el ruteo jerárquico entre redes y subredes; además, soporta más niveles jerárquicos que IPv4 y en este aspecto es semejante a la dirección IPv6.

Los últimos 6 bytes de la dirección se asignan para el campo del **identificador del sistema terminal** (ESI, End System Identifier). Este campo desempeña el mismo papel de la dirección MAC del nodo ATM. Su formato también corresponde al de la dirección MAC.

La dirección ESI es asignada al nodo terminal por el fabricante del equipo de acuerdo con las reglas de la IEEE. Esto significa que los primeros 3 bytes contienen el código del fabricante, mientras que los 3 bytes restantes son el número de serie, cuya unicidad debe asegurar el fabricante.

Cuando se trabaja en una red privada ATM, el formato de dirección corresponde por lo regular al formato E.164 con modificaciones menores.

Cuando el nodo terminal está conectado al switch ATM, lleva a cabo el denominado *procedimiento de registro*. El nodo terminal informa de su dirección ESI al switch y este último informa respecto a la parte más significativa de la dirección al nodo terminal, es decir, el número de la red a la cual está conectado ese nodo.

Además de la parte de la dirección, el nodo terminal utiliza el paquete de establecimiento de llamada del protocolo Q.2931 para solicitar que se forme una conexión virtual e incluir las partes que describen parámetros de tráfico y requerimientos de QoS. Cuando un paquete así llega al switch, éste debe analizar dichos parámetros y decidir si tiene suficientes recursos de rendimiento para dar servicio a una nueva conexión virtual. Si es así, se aceptará una nueva conexión virtual y el switch pasará el paquete de establecimiento de llamada de acuerdo con la dirección de destino y la tabla de ruteo. Si los recursos disponibles no son suficientes, se denegará la solicitud.

21.5.5 Categorías de servicios de protocolos de ATM y control de tráfico

Con el fin de soportar la QoS requerida para diversas conexiones virtuales y asegurar el uso racional de los recursos de la red, la red ATM pone en marcha varios servicios de capa ATM relacionados con el servicio del tráfico del usuario. Éstos son servicios internos de la red ATM, diseñados para soportar el tráfico del usuario o clases diferentes con protocolos AAL. No obstante, en contraste con los protocolos AAL que funcionan en nodos terminales, tales servicios están distribuidos sobre todos los switches de la red y se clasifican en categorías, lo cual corresponde generalmente a las clases de tráfico que llegan a la entrada

de la capa AAL del nodo terminal. Los servicios de capa ATM son solicitados por el nodo terminal a través de UNI y se emplea el protocolo Q.2931 cuando se establece una conexión virtual. Como en el caso de una solicitud para AAL, cuando se solicita el servicio es necesario especificar su categoría, tráfico y parámetros de QoS. Estos parámetros se toman de los parámetros semejantes de la capa AAL o se definen como valores predeterminados según la categoría del servicio.

Existen cinco categorías de servicio de la capa de protocolo ATM y son soportadas por los servicios con los mismos nombres:

- **CBR** (Constant Bit Rate, velocidad constante de bits): servicios de tráfico CBR.
- **rtVBR** (real-time Variable Bit Rate, velocidad variable de bits en tiempo real): servicios para tráfico VBR, lo cual requiere una velocidad promedio de datos constante y la sincronización entre el transmisor y el receptor.
- **nrtVBR** (not real-time Variable Bit Rate, velocidad variable de bits en tiempo no real): servicios para tráfico VBR, lo cual requiere la observancia de la velocidad promedio de datos, pero no la sincronización del transmisor y el receptor.
- **ABR** (Available Bit Rate, velocidad de bits disponible): servicios para tráfico VBR, lo cual requiere una velocidad mínima de datos y no necesita que se sincronicen el transmisor y el receptor.
- **UBR** (Unespecified Bit Rate, velocidad de datos no especificada): servicios para tráfico, los cuales no proporcionan ningún requerimiento de la velocidad de transmisión de datos, ni sincronizan al transmisor y al receptor.

Los nombres de la mayoría de las categorías de servicio coinciden con los de los tipos de tráfico del usuario para los cuales se diseñaron aquéllas. Sin embargo, es necesario comprender que los servicios de capa ATM son mecanismos internos de la red ATM ocultos de las aplicaciones por medio de la capa AAL.

Los *servicios CBR* están destinados a soportar el tráfico de las aplicaciones sincrónicas: voz, simulación de líneas rentadas digitales y así sucesivamente. Cuando una aplicación establece la conexión de la categoría CBR, solicita la velocidad pico de las celdas (PCR), la cual es la velocidad máxima que puede soportar la conexión sin el riesgo de pérdida de celdas. La aplicación también solicita los siguientes parámetros de QoS: CTD, CDV y CLR.

En ese sentido, los datos se transmiten a través de esta conexión a la velocidad solicitada, la cual no es más grande y, en la mayoría de los casos, tampoco es más pequeña que la solicitada, aunque es posible la reducción de velocidad, por ejemplo, cuando se transmite voz comprimida utilizando la categoría de servicio CBR. Cualquier celda transmitida por la estación a una velocidad superior se controla mediante la primera red conmutada y es marcada con el atributo CLP = 1. Cuando se presenta congestión de la red, tales celdas pueden ser descartadas por la red. Las celdas retrasadas y que no caben en el intervalo acordado por el parámetro CDV también se consideran de baja prioridad y están marcadas con el atributo CLP = 1.

Para conexiones CBR, no existen limitaciones para cierta discontinuidad de la PCR solicitada a diferencia de, por ejemplo, en los enlaces T1/E1, en los que la velocidad debe ser un múltiplo de 64 kbps.

En comparación con los servicios CBR, los *servicios VBR* requieren procedimientos más complicados para solicitar la conexión entre la red y la aplicación. Además de la PCR, la aplicación VBR solicita otros dos parámetros: SCR, que es una velocidad promedio de transmisión de datos permitida para la aplicación, y MBS. MBS es medida por el número de celdas ATM;

no obstante, el usuario debe exceder la velocidad del umbral PCR sólo por periodos breves, durante los cuales se transmite el volumen de datos que no exceda MBS. Este periodo se conoce como **tolerancia de ráfaga** (BT, Burst Tolerance). La red calcula este periodo como un valor derivado según los tres parámetros especificados: PCR, SCR y MBS.

Si la PCR es monitoreada durante un periodo más largo que la BT, las celdas se marcarán como violatorias del acuerdo del servicio: el atributo CLP se establece a 1.

Para los *servicios rtVBR*, se establecen los mismos parámetros de QoS que para los servicios CBR, y los servicios nrtVBR están limitados únicamente por el soporte de los parámetros de tráfico. Para ambas categorías de tráfico VBR, la red soporta cierto nivel de la CLR, que se especifica explícitamente cuando se establece una conexión o se elige como un valor predeterminado para determinada clase de tráfico.

Para controlar el tráfico y los parámetros QoS, ATM utiliza el denominado *algoritmo de velocidad de celdas genérico*, que puede verificar si el usuario observa el acuerdo respecto a parámetros tales como PCR, CDV, SCR, BT, CTD y CDV. Funciona con base en el algoritmo de fuga de cubeta modificado empleado en la tecnología Frame Relay.

Para muchas aplicaciones que tienen múltiples ráfagas en relación con el tráfico que generan, es imposible predecir los parámetros de tráfico acordados cuando se establece una conexión. Por ejemplo, son impredecibles el procesamiento de transacciones y el tráfico entre dos LANs en comunicación. Las variaciones de intensidad del tráfico son tan grandes que es imposible concluir cualquier acuerdo razonable con la red.

En contraste con los servicios CBR y ambos servicios VBR, *el servicio UBR* no soporta parámetros de tráfico o parámetros de QoS. UBR ofrece solamente entrega con el mejor esfuerzo sin garantías. Como ha sido diseñado especialmente para cuando se exceden los límites del ancho de banda, el servicio UBR da una solución parcial para aplicaciones de ráfagas impredecibles que no están listas para concluir ningún acuerdo relacionado con los parámetros del tráfico.

Las principales desventajas del servicio UBR son la carencia de mecanismos de control de flujo y la incapacidad para tener en cuenta otros tipos de tráfico. Las conexiones UBR continuarán la transmisión de datos incluso en casos de congestión de la red. Los switches de la red pueden almacenar temporalmente algunas celdas del tráfico entrante; sin embargo, llegará el momento en que se presentará una sobrecarga del búfer o memoria temporal y las celdas se perderán. Como no hay acuerdo acerca del tráfico o parámetros QoS para las conexiones UBR, sus celdas son las primeras en descartarse.

El *servicio ABR*, similar al UBR, permite exceder el ancho de banda; sin embargo, debido a las técnicas de control de tráfico, asegura un transporte confiable y proporciona algunas garantías para la entrega de las celdas.

> ABR es el primer tipo de servicio de capa ATM que asegura transporte confiable para el tráfico en ráfagas, debido a su capacidad para hallar espacios de tiempo no utilizados en el tráfico de red común y llenarlos con sus celdas, a condición de que dichos espacios no sean necesarios para otras categorías de servicio.

De manera similar a los servicios CBR y VBR, cuando se establece una conexión de categoría ABR, es necesario ponerse de acuerdo en el parámetro PCR. No obstante, no se concluyen acuerdos respecto a parámetros de transmisión de celda o parámetros de ráfaga. En su lugar, la red y el nodo terminal concluyen el acuerdo acerca de la velocidad de transmisión mínima requerida: la MCR. Para la aplicación que se realiza en el nodo terminal, esto garantiza un ancho de banda pequeño, por lo regular el mínimo requerido para la operación normal de

esa aplicación. Cuando se concluye dicho acuerdo, el nodo terminal conviene no transmitir datos a velocidades que excedan la PCR, y la red acuerda asegurar siempre la MCR.

Si los valores de las velocidades tanto máxima como mínima no se han especificado cuando se concluye una conexión ABR, entonces, de manera predeterminada, se considera que el enlace PCR coincide con la velocidad de la línea de acceso que proporciona acceso a la estación terminal a la red y el valor predeterminado de MCR es igual a cero.

El tráfico de la conexión ABR obtiene QoS garantizada en cuanto a la repartición de celdas perdidas y el ancho de banda disponible. En la medida en que se relaciona con los retardos de transmisión de celda, no se garantiza, aunque la red hace su mejor esfuerzo para reducirlo a un mínimo. En consecuencia, el servicio ABR no es el más adecuado para aplicaciones en tiempo real, cuyos flujos de datos sean altamente sensibles a los retardos de transmisión.

Cuando se transmite tráfico CBR, VBR y UBR, se pierde el control explícito sobre la congestión de la red. En su lugar, se utiliza el mecanismo basado en el descarte de las celdas violatorias. Al mismo tiempo, los nodos que usan los servicios CBR y VBR hacen su mejor esfuerzo para no violar el contrato de tráfico. Si lo logran, arriesgan celdas disponibles. Debido a esto, por lo regular no utilizan ancho de banda adicional incluso si está disponible.

El servicio ABR permite usar las reservas de ancho de banda porque utiliza el mecanismo de retroalimentación para informar al nodo terminal que la reserva de ancho de banda está disponible. Dicho mecanismo puede ayudar al servicio ABR a reducir la velocidad de transmisión de los datos del nodo terminal en la red para la MCR en el caso de la congestión de la red.

El nodo que utiliza el servicio ABR debe enviar de manera periódica **celdas especiales de administración de recursos (**RM**,** por las siglas para **Resource Management)** con las celdas de datos. Las celdas de RM que el nodo envía a través del flujo de datos son celdas de **administración de recursos dirigidos hacia delante** (FRM, Forward Resource Management), mientras que las celdas que viajan en la dirección inversa son celdas de **administración de recursos dirigidos hacia atrás** (BRM, Backward Resource Management).

Existen varios **ciclos** o **loops de retroalimentación**. El más simple existe entre dos estaciones terminales. Cuando está presente, el switch de la red informa a la estación terminal acerca de la congestión, para lo cual emplea una bandera especial en el campo del control de congestión directo (la bandera EFCI) de la celda de datos conducida por el protocolo ATM. Luego, la estación terminal envía un mensaje especial a través de la red. Este mensaje se halla contenido en una celda especial BRM, la cual informa a la estación de origen que es necesario reducir la velocidad a la que envía las celdas en la red.

Cuando se aplica dicho método, la estación terminal mantiene la responsabilidad principal para el control del flujo, mientras que el switch desempeña el papel pasivo en la retroalimentación e informa únicamente a la estación emisora respecto a la congestión.

Un método así de simple tiene varias desventajas obvias. La estación terminal no obtiene información del mensaje BRM relacionado con el valor con el que es necesario reducir la velocidad a la cual envía los datos en la red. Por lo tanto, disminuirá la velocidad al valor mínimo, la MCR, aunque quizá una reducción así de significativa no sea necesaria. Además, en una red extensa, los switches deben continuar almacenando datos temporalmente durante todo el intervalo hasta que la notificación sobre la congestión viaje a través de la red. Adviértase que para las WAN, este periodo puede ser extenso. Así, puede presentarse una sobrecarga del búfer o memoria temporal, de manera que no se conseguirá el efecto deseado.

Existen otros métodos más complejos de control de flujo. En estos métodos, los switches desempeñan un papel más activo y se proporciona al nodo emisor información más detallada acerca de la velocidad de datos que puede soportarse.

En el primer método, el nodo de origen envía una celda FRM que especifica el valor de la velocidad de datos que es capaz de soportar. Cada conmutador o switch, por el cual ha pasado este mensaje conforme viaja a lo largo del circuito virtual, puede reducir la velocidad solicitada al valor específico que puede soportar de acuerdo con la cantidad de recursos disponibles; también puede dejar sin cambios la velocidad solicitada. El nodo de destino, una vez que ha recibido la celda FRM, la convierte en la celda BRM y la envía en la dirección inversa. Obsérvese que también puede reducir la velocidad solicitada. En cuanto ha recibido una respuesta en la celda BRM, el nodo de origen sabe exactamente cuál velocidad de datos está disponible para aquélla.

En el segundo método, cada switch de red puede funcionar como el nodo de origen y como el nodo de destino. Como el primero, puede generar celdas FRM y enviarlas sobre los circuitos virtuales existentes. Como el segundo, puede enviar celdas BRM en la dirección inversa con base en el contenido de las celdas FRM recibidas. Este método es más rápido y más adecuado para redes a largas distancias.

Como se aprecia en la descripción, el servicio ABR está destinado para algo más que soportar directamente requerimientos de QoS para una conexión virtual específica. También es apropiado para una distribución de recursos más racional entre los suscriptores de la red, lo que, a la larga, mejora la calidad de los servicios proporcionados a todos los suscriptores de la red.

Los switches ATM utilizan varios mecanismos para soportar la QoS requerida. Aparte de los mecanismos descritos en los estándares ITU-T y ATM Forum, según los cuales los acuerdos sobre tráfico y los parámetros de QoS están concluidos y las celdas que violan estos acuerdos son descartadas, prácticamente todos los fabricantes de equipo ATM implementan varias colas de celdas servidas con diferentes prioridades.

La estrategia basada en prioridades para el servicio al tráfico se basa, a su vez, en las categorías de servicio para cada conexión virtual. Antes de adoptar la especificación ABR, la mayoría de los switches ATM ponía en práctica diseños de servicio simple de capa única, que daba la prioridad más alta al tráfico de CBR, la segunda prioridad a la de VBR y la tercera a la de UBR. De acuerdo con tal diseño, la combinación de CBR y VBR puede paralizar el tráfico servido por otra clase de servicios. Un diseño así no trabajaría correctamente con el tráfico ABR, debido a que no aseguraría sus requerimientos para una velocidad mínima de transmisión de celdas. Con el fin de asegurar que este requerimiento ha sido satisfecho, es necesario asignar algún ancho de banda garantizado.

Para soportar el servicio ABR, los switches ATM deben poner en marcha un diseño de servicio de dos capas que satisfaga los requerimientos de CBR, VBR y ABR. De acuerdo con este diseño, el switch proporciona alguna parte de ancho de banda a cada clase de servicio. El tráfico de CBR obtiene alguna parte del ancho de banda requerido para soportar la PCR, el tráfico de VBR consigue alguna parte del ancho de banda que se necesita para soportar la SCR y el tráfico de ABR adquiere la parte del ancho de banda suficiente para asegurar la MCR. Esto garantiza que cada conexión puede funcionar sin pérdidas de celdas y no entregará celdas ABR a costa del tráfico de CBR o VBR. En la segunda capa de este algoritmo, el tráfico CBR y VBR puede apoderarse del ancho de banda restante, si es necesario, porque las conexiones ABR ya tienen el ancho de banda mínimo garantizado para ellas.

Una tarea por separado que debe resolverse para soportar el funcionamiento correcto de los servicios descritos y asegurar el nivel especificado de QoS para todas las clases de tráfico consiste en hacer óptima la operación de la red ATM mediante el uso de métodos de ingeniería de tráfico. Aplicar la técnica del circuito virtual en redes ATM (así como también Frame Relay) proporciona buenos requisitos previos para resolver el problema de ingeniería de tráfico. Sin embargo, aún no existen procedimientos automatizados para la selección dinámica de

rutas para circuitos virtuales a fin de asegurar una carga de red equilibrada. Todo el trabajo relacionado con la optimización de las rutas debe llevarse a cabo con antelación, para lo cual se debe emplear algún software de terceros para simulación u optimización de la red.

En redes ATM, la selección de la ruta para circuitos virtuales y trayectorias virtuales puede efectuarse mediante el uso del protocolo de enrutamiento PNNI que tiene en cuenta no sólo el ancho de banda nominal de los enlaces, sino también el ancho de banda disponible para establecer nuevos circuitos virtuales.

RESUMEN

- La técnica del circuito virtual consiste en separar las operaciones de ruteo y conmutación de paquetes. El primer paquete de tales redes contiene la dirección del suscriptor invocado y crea una trayectoria virtual en la red mediante la configuración de switches de tránsito. Los otros paquetes parten a través del circuito virtual en el modo de conmutación con base en el número del circuito virtual.
- Las ventajas de la técnica del circuito virtual son la conmutación rápida de paquetes de acuerdo con el número del circuito virtual, así como la reducción del campo de dirección del paquete y, en consecuencia, la disminución de la redundancia del encabezado. Las desventajas incluyen la imposibilidad del flujo de datos en paralelo entre dos suscriptores mediante dos rutas alternativas y la ineficacia de establecer una trayectoria virtual para flujos de datos a corto plazo.
- Las redes X.25 son las tecnologías WAN más antiguas y mejor probadas. La pila de protocolo de tres capas de X.25 funciona bien en enlaces de comunicaciones ruidosos y no confiables al corregir errores y controlar el flujo de datos en las capas del paquete y enlaces de datos.
- La mayoría de las primeras redes Frame Relay soportaban sólo circuitos virtuales permanentes (PVC). Recientemente se diseñaron y llegaron a utilizarse los circuitos virtuales conmutados (SVC).
- Las redes Frame Relay se crearon para transmitir tráfico computacional en ráfagas. Por lo tanto, en el transcurso de la reservación de ancho de banda es necesario especificar la velocidad promedio del tráfico, la CIR y el tamaño de la ráfaga coordinado, B_c.
- La tecnología ATM es un diseño adicional de las ideas acerca de reservar el ancho de banda del circuito virtual con antelación, lo cual se puso en práctica por primera vez en la tecnología Frame Relay.
- ATM soporta los principales tipos de tráfico típico para diferentes tipos de suscriptores, incluido el tráfico CBR, típico para redes de telefonía y redes de difusión de vídeo, y el tráfico VBR, típico para redes computacionales y empleado cuando se transmite vídeo o voz con compresión.
- Para cada tipo de tráfico, el usuario puede solicitar de la red varios parámetros de QoS, incluidos la velocidad máxima de bits (PCR), la velocidad promedio de bits (SCR), la ráfaga máxima (MBS) y diversos parámetros que controlan relaciones de tiempo entre el transmisor y el receptor, que son importantes para el tráfico sensible al retardo.
- La tecnología ATM por sí misma no define nuevos estándares de capa física. Por el contrario, utiliza los existentes. El principal estándar para la tecnología ATM es la capa física de SONET/SDH y PDH.

PREGUNTAS DE REPASO

1. ¿Qué parámetros pueden usarse para describir un circuito virtual?
2. ¿Qué debería hacerse en caso de falla del enlace físico a través del cual pasa el circuito virtual?
3. Enumere las etapas principales para establecer un circuito virtual.
4. ¿Puede funcionar una red X.25 sin PAD?
5. ¿Qué puede ocurrir al tráfico del mejor esfuerzo si el tráfico prioritario que llega a la interfase de entrada Frame Relay no está limitado por la intensidad promedio?
6. ¿Cómo puede conectarse el usuario al PAD interconstruido mediante la red telefónica, siempre que trabaje en una terminal que no soporte llamadas automáticas a través de la red telefónica?
7. Si su compañía necesita conectar redes de oficina remota múltiple a la red central y a otra pero usted sólo ha rentado enlaces analógicos con módems sincrónicos instalados de 19.2 Kbps, ¿cuál tecnología elegiría usted: X.25, Frame Relay o ATM? Justifique su solución y explique los factores que influyeron en ella.
8. ¿Cuál función del algoritmo de cubeta de estafetas no está soportada por el algoritmo de cubeta con fuga?
9. ¿Qué categoría de servicios es conveniente elegir para transmitir voz al usar la red ATM?
10. ¿Cuántos circuitos virtuales es necesario establecer en cada dirección entre cada par de switches ATM, siempre que usted necesite transmitir tres clases de tráfico con diferentes niveles de QoS?
11. ¿Para qué categoría de servicio la red ATM controla explícitamente el flujo de datos?, ¿por qué no utiliza control del flujo para otros tipos de servicios?
12. Suponga que usted necesita establecer manualmente una PVC en dos amplias redes ATM empresariales conectadas mediante una red ATM pública. Usted no necesita que sus números VCI dependan de los números VCI empleados por el administrador de la red ATM pública. ¿Qué clase de conmutación solicitaría del proveedor de servicio ATM pública?
13. Suponga que ha conectado dos LANs mediante la operación de un puente remoto en el que utiliza un PVC en la red Frame Relay. Las sesiones NetBEUI entre computadoras pertenecientes a distintas redes se interrumpen a menudo. Cuando las computadoras pertenecen a la misma LAN, no hay tales problemas. ¿Qué razones pueden provocar esta situación?

PROBLEMAS

1. Compare el número de tramas generadas al intercambiar dos mensajes TCP (al enviar los datos y al recibir un acuse de recibo) entre dos hosts terminales conectados mediante un switch, cuando éste es un X.25 y cuando es un Frame Relay.
2. ¿En cuál caso será mayor el porcentaje de las tramas entregadas al nodo de destino al usar la red Frame Relay: cuando el servicio se solicite con base en los parámetros *CIR*, *B* y B_e o cuando el servicio se solicita únicamente de acuerdo con *CIR* y B_c (se supone que los valores de *CIR* y B_c para ambos casos son los mismos)? Suponga que la red Frame Relay está subutilizada y que el nodo emisor envía los datos a una velocidad que a menudo excede de manera significativa el valor CIR.

3. Supóngase que el switch Frame Relay y el switch IP están basados en la misma arquitectura y procesadores con la misma velocidad de reloj. ¿Proporcionará el switch Frame Relay mejor rendimiento que el ruteador IP? Justifique su opinión.

4. Resuelva la tarea de ingeniería de tráfico para la red ATM que se muestra en la figura 21.12. Debe asegurarse la carga más uniforme para todos los recursos de la red para la carga ofrecida proporcionada en la figura 21.13.

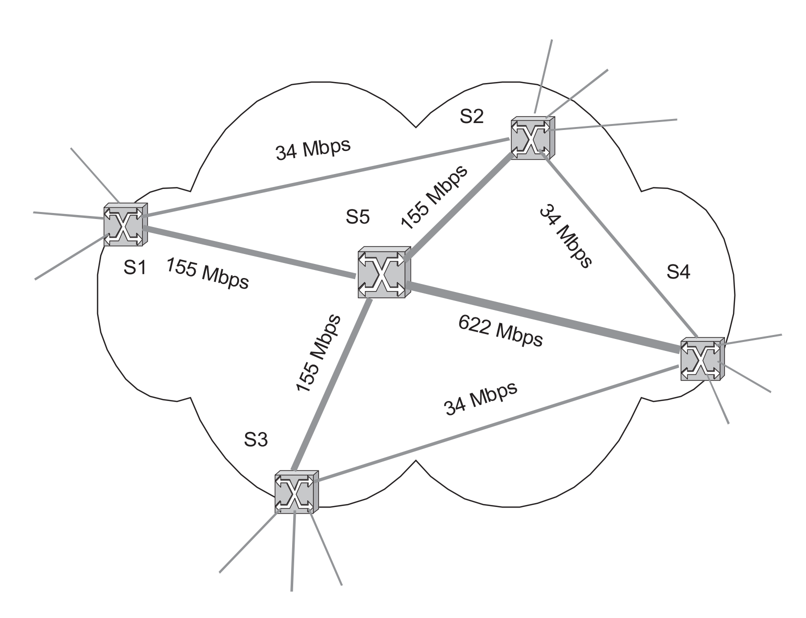


FIGURA 21.12 Red ATM.

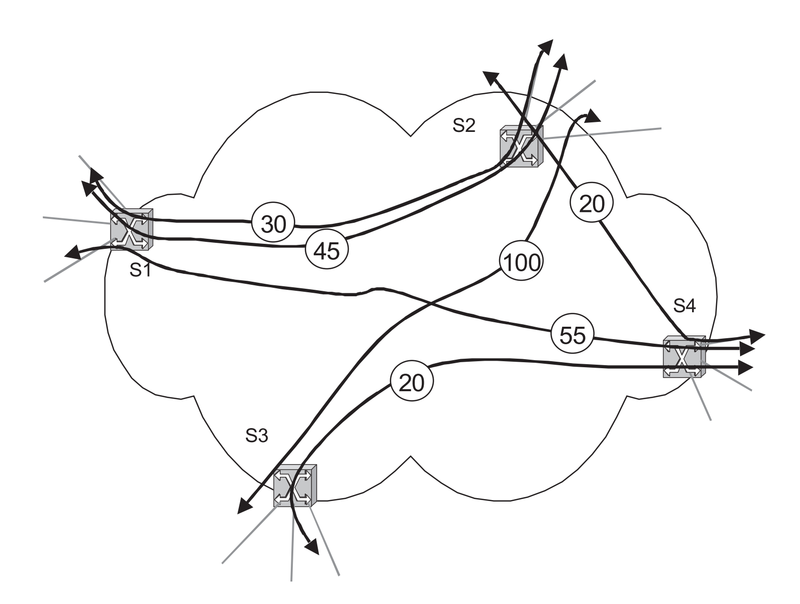


FIGURA 21.13 Carga ofrecida.

CONCLUSIÓN: MIRANDO HACIA EL FUTURO

Cuanto más miramos hacia el futuro, menos tenemos oportunidad de ver las redes computacionales en el sentido tradicional de este término, en otras palabras: las redes que transmiten solamente texto y número. La tendencia para todo tipo de redes, ya sean telefónicas, computacionales o basadas en la TV, es la convergencia. Incluso ahora, las redes computacionales transmiten tipos de tráfico que al inicio no eran típicos de ellas. Esto se considera de varias formas: como conversaciones interactivas tradicionales entre suscriptores de una red telefónica, como la difusión por demanda (ya sea de música o de entrevistas o conversaciones grabadas previamente) sobre Internet y como correo de voz. La transmisión de imágenes requiere una tasa de transferencia mucho más alta y, por lo tanto, es menos común. Sin embargo, incluso a una velocidad de acceso de aproximadamente 64-128 Kbps, es posible visualizar una teletransmisión en una pequeña ventana rectangular en la pantalla de la PC.

Así, las redes de telecomunicaciones del futuro son igualmente capaces de transmitir ráfagas de tráfico de datos y flujos de sonido o video. Las redes del futuro heredarán las mejores características de sus predecesores: redes computacionales y telefónicas, además de las redes de difusión de radio o televisión; empero, utilizarán una tecnología de transporte común que debe asegurar la transmisión de cada tipo de tráfico con la QoS requerida. Tal tecnología, de acuerdo con la opinión común de la mayoría de los especialistas, debe basarse en la técnica de conmutación de paquetes y utilizar ampliamente el protocolo ganador: IP. Esto crea redes del futuro similares a las redes computacionales contemporáneas; no obstante, se esperan innovaciones tecnológicas significativas.

La lista de tales innovaciones tecnológicas probablemente incluirá dispositivos terminales de tipos más novedosos, que combinarían la potencia funcional de una PC con la simplicidad y facilidad de uso típicas de un equipo telefónico. Los teléfonos inteligentes ("Smartphones") y los PDA son prototipos de esos dispositivos. La llegada de un dispositivo de esta naturaleza que permitiese a sus usuarios tener acceso a páginas web predefinidas al presionar varias teclas o botones, organizar una conferencia telefónica, enviar un mensaje de correo electrónico con aplicaciones multimedia, o solicitar una demostración de video bajo demanda (además de tener acceso a muchos más servicios de los que existen sólo como proyectos) serviría como un incentivo para que las telecomunicaciones evolucionen.

La tecnología de las rutas virtuales controladas con base en los estándares DWDM y MPLS generalizados (GMPLS) llegará a ser la respuesta para el crecimiento de la demanda para el transporte de súper alta velocidad y gran calidad. El núcleo de la nueva red pública de telecomunicaciones estará basado en cables de fibra óptica múltiple, que asegurarían la tasa de transferencia de varios terabytes entre nodos de comunicación. Este núcleo también creará las bases para la transmisión de cantidades de información que parecen un sueño inalcanzable en la actualidad. Para propósitos económicos, el núcleo debe soportar conmutación de solamente flujos de datos de súper-alta velocidad, como el flujo de datos de sólo una longitud de onda específica (conmutación DWDM) y de incluso el flujo de sólo un núcleo individual, sin unidades de conmutación más pequeñas. Como resultado, la tecnología SDH se trasladará fuera del núcleo de la red y desempeñará el papel de una red de

acceso para conmutadores DWDM. Otro logro revolucionario será el control del núcleo de las redes con base en la tecnología GMPLS, cuando las trayectorias de los núcleos miembro, longitudes de onda y contenedores SDH se crearían dinámicamente al utilizar el protocolo de señalización unificado. El asunto más importante es que también habría una versión para el usuario final de este protocolo. Esto significa que el suscriptor del núcleo (por ejemplo, el proveedor del servicio) sería capaz de usar con flexibilidad la tasa de transferencia, según las necesidades actuales.

Por el momento, una tasa o velocidad de acceso baja, especialmente para la comunidad de suscriptores más amplia, es uno de los principales obstáculos para el uso extendido de los nuevos servicios multimedia. Existen varias soluciones a este problema, incluido el uso de circuitos locales de cobre existentes (el enfoque más adecuado para la mayoría de los usuarios individuales), la adopción del acceso inalámbrico (tanto fijo como móvil) y la instalación de circuitos locales ópticos mediante el uso de una tecnología de red óptica pasiva económica. Las tecnologías ATM o IP/MPLS se emplearán para compartir el ancho de banda del canal.

A pesar de un considerable ascenso en el rendimiento tanto del núcleo de la red como de las redes de acceso, todavía son posibles los bloqueos del tráfico cuando éste excede simultáneamente la capacidad de las colecciones de redes. Por lo tanto, para la transmisión de tráfico de alta calidad, las redes del futuro usarán ampliamente métodos de soporte de QoS. En el núcleo de la red, éstos serán métodos que garanticen el servicio a grandes flujos de datos agregados que conducen datos para un gran número de suscriptores, en otras palabras, métodos cercanos a DiffServ, que empieza a encontrar la aplicación en redes portadoras. En redes de acceso, métodos similares a los utilizados en las tecnologías ATM e IntServ darán servicio a flujos individuales.

También cambian las LAN. El cable pasivo que conecta computadoras se reemplaza por diversos equipos de comunicaciones, como conmutadores, ruteadores y compuertas. Debido a este equipo, se han podido construir grandes redes corporativas al conectar millares de computadoras a través de una complicada estructura. Se ha vuelto a generar el interés en grandes “mainframes” o supercomputadoras, debido principalmente a que, después de disminuir la euforia causada por la facilidad de trabajar con PC, los sistemas que constan de millares de servidores son más difíciles de mantener que varias computadoras grandes. De este modo, en el nuevo giro de la espiral evolutiva, las empresas han vuelto a instalar microcomputadoras. Sin embargo, esta vez han llegado a ser miembros completos de la red, que soportan tanto tecnología Ethernet como Token Ring, además de la pila TCP/IP que, debido a Internet, llegó a ser el estándar de facto.

Las anteriores sólo son algunas líneas de desarrollo para las redes de telecomunicaciones, que resultan claramente visibles incluso desde ahora.

REFERENCIAS Y LECTURAS RECOMENDADAS

CONTENIDO

LECTURAS RECOMENDADAS PARA LA PARTE I

1. Armitage, G., *Quality of Service in IP Networks,* Pearson Education, 2000.
2. Black, U., *Internet Security Protocols: Protecting IP Traffic,* 1a. ed., Prentice Hall, 2000.
3. Black, U., *Emerging Communications Technologies,* 2a. ed., Prentice Hall Professional, 1997.
4. Black, U., *Data Networks: Concepts, Theory and Practice,* Englewood Cliffs, New Jersey: Prentice Hall, 1989.
5. Comer, D.E., *Internetworking with TCP/IP,* vol. 1, *Principles, Protocols, and Architecture,* 3a. ed., Prentice Hall, 2000.
6. Comer, D.E. y Stevens, D., *Internetworking with TCP/IP,* vol. 2, *Design Implementation, and Internals,* Prentice Hall, 1994.
7. Comer, D.E., Stevens, D., *Client-Server Programming and Applications,* Prentice Hall, 2001.
8. Dodd, A.Z., *The Essential Guide to Telecommunications 1*, 2a. ed., Prentice Hall, 1999.
9. Dorogovtsev, S.N. y Ferreira Mendes, J.F., *Evolution of Networks: From Biological Nets to the Internet and WWW,* Oxford University Press, 2003.
10. Fitzgerald, J., *Business Data Communications,* John Wiley & Sons, 1993.
11. Ford, W., *Computer Communications Security,* Prentice Hall, 1994.
12. Freeman, R., *Telecommunications Transmission Handbook,* Nueva York: Wiley, 1998.
13. Halsall, F., *Data Communications, Computer Networks, and Open Systems,* Addison-Wesley, 1996.
14. Hamacher, C.V., Vranesic, Z.G. y Zaky, S.G., *Computer Organization,* Nueva York: McGraw Hill, 1984.
15. Hardy, W. C., *QoS Measurement and Evaluation of Telecommunications Quality of Service,* John Wiley & Sons, 2001.
16. Hauben, M., Hauben, R. y Truscott, T., *Netizens: On the History and Impact of Usenet and the Internet,* 1a. ed., Wiley-IEEE Computer Society Pr., 1997.
17. Ibe, O.C., *Converged Network Architectures: Delivering Voice and Data Over IP, ATM, and Frame Relay,* Wiley, 2001.
18. Keshav, S., *Efficient Implementation of Fair Queuing,* Proceedings of the ACM SIGCOMM, 1990.
19. Keshav, S., *An Engineering Approach to Computer Networking,* Addison Wesley, 1997.
20. Kleinrock,L., *Queuing Systems,* vol. 1, *Theory,* Wiley-Interscience, 1975.
21. Kurose, J.F. y Ross, K.W., *Computer Networking: A Top-Down Approach Featuring the Internet*, 3a. ed., Addison Wesley, 2004.
22. LaQuey, T., *The Internet Companion: A Beginner's Guide to Global Networking,* Reading, Massachusetts: Addison-Wesley, 1994.
23. Leiner, B.M., Cerf, V.G. y cols., *Brief History of the Internet,* Internet Society (ISOC), **www.isoc.org/internet/history/brief.shtml.**
24. León-García A. y Widjaja, I., *Communication Networks: Fundamental Concepts and Key Architectures,* 1a. ed., McGraw-Hill Science/Engineering/Math, 200l.
25. Le Boudec, J.-Y. y Thiran, P., "Network Calculus. A Theory of Deterministic Queuing Systems for the Internet Series: Lecture Notes", en *Computer Science,* vol. 2 050, 2001.
26. Null, L. y Lobur, J., *The Essentials of Computer Organization and Architecture Dimensions,* Jones & Bartlett Pub., 2003.
27. Osborne, E. y Ajay, S., *Traffic Engineering with MPLS,* Cisco Press, 2002.
28. Peterson, L.L. y Davie, B.S., *Computer Networks: A Systems Approach,* 3a. ed., Morgan Kaufmann, 2003.

29. Rose, M.T., *The Open Book: A Practical Perspective* on *OSI*, Englewood Cliffs, New Jersey: Prentice Hall, 1990.
30. Rowe, S.H., *Telecommunications for Managers,* 3a. ed., Prentice Hall, 1995.
31. Stallings, W., *Data and Computer Communications,* 7a. ed., Prentice Hall, 2003.
32. Stallings, W., *Wireless Communications and Networks,* Prentice Hall, 2002.
33. Stallings, W., *Local and Metropolitan Area Networks,* Macmillan Publishing Company, 1993.
34. Standards, International Organization for Standardization, Information Processing System — *Open System Interconnection: Specification of Abstract Syntax Notation One (ASN.1)*, International Standard 8824, 1987.
35. Stevens, R.W., *TCP/IP Illustrated, vol.* 1, *The Protocols,* la. ed., Addison-Wesley Professional, 1993.
36. Young Moo Kang, Miller, B.R. y Pick, R.A., *Comments* on *"Grosch's law re-revisited: CPU power and the cost of computation",* comunicaciones del ACM, vol. 29, emisión 8, 1986.
37. Zheng Wang, *Internet QoS: Architectures and Mechanisms for Quality of Service,* 1a. ed., Morgan Kaufmann, 2001.
38. Zwcky, E.D., Cooper, S. y Chapman, B.D., *Building Internet Firewalls,* O'Reilly, 2000.

LECTURAS RECOMENDADAS PARA LA PARTE II

1. Abbas, J., *The Wireless Mobile Internet,* John Wiley & Sons, 2003.
2. Ashwin, G., *DWDM Network Designs and Engineering Solutions,* Pearson Education, 2002.
3. Bertsekas, D. y Gallager, R., *Data Networks,* 2a. ed., Prentice Hall, 1992.
4. Black, U., *Physical Level Interfaces and Protocols,* Los Alamitos, California: IEEE Computer Society Press, 1988.
5. Couch, L.W., *Digital and Analog Communication Systems,* 6a ed., Prentice Hall, 2001.
6. EIA232E p: *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange,* revisado de EIA232D, julio de 1991.
7. Gibson, J.D., *Principles of Digital and Analog Communications,* 2a. ed., Prentice Hall, 1993.
8. Halsall, F., *Data Communications, Computer Networks, and Open Systems,* Addison Wesley, 1996.
9. Haykin, S., *Digital Communications,* Wiley, 1988.
10. Nicopolitidis, P., Obaidat, M.S. y cols., *Wireless Network,* Wiley, 2003.
11. Proakis, J.G., *Digital Communications,* 4a. ed., McGraw-Hill, 2001.
12. Rowe, S.H., *Telecommunications for Managers,* 3a. ed., Prentice Hall, 1995.
13. Sexton, M. y Reid, A., *Broadband Networking: ATM, SDH, and SONET,* Artech House, 1997.
14. Shu Lin y Costello, D.J., *Error Control Coding,* 2a. ed., Prentice Hall, 2004.
15. Sklar, B., *Digital Communications: Fundamentals and Applications,* 2a. ed., Prentice Hall PTR, 2001.
16. Stallings, W., *Data and Computer Communications,* 6a. ed., Prentice Hall, 2004.
17. Stallings, W., *Wireless Communications and Networks,* Prentice Hall, 2002.
18. Sweeney, P., *Error Control Coding,* Wiley, 2002.
19. Wicker, S.B., *Error Control Systems for Digital Communication and Storage,* Prentice Hall, 1995.

20. Wirth, N., *Digital Circuit Design for Computer Science Students. An Introductory Textbook,* Springer Verlag, 1995.
21. Zeimer, R.E. y Peterson, R.L., *Introduction to Digital Communication,* Prentice Hall, 2001.

LECTURAS RECOMENDADAS PARA LA PARTE III

1. Abbas, J., *The Wireless Mobile Internet,* John Wiley & Sons, 2003.
2. Bertsekas D. y Gallager, R., *Data Networks,* 2a. ed.,Prentice Hall, 1992.
3. Black, U., *Data Networks: Concepts, Theory and Practice,* Englewood Cliffs, New Jersey: Prentice Hall, 1989.
4. Bux, W., *Local-area Subnetworks: A Performance Comparison,* IEEE Press Trans. Comm., vol. COM-29, emisión 10, 1981.
5. Cunningham,D., Lane, W.G. y Lane, B., *Gigabit Ethernet Networking,* 1a. ed., Sams, 1999.
6. Gast M. y Gast, M.S., *802.11 Wireless Networks: The Definitive Guide,* 1a. ed., O'Reilly, 2002.
7. Halsall, F., *Data Communications, Computer Networks, and Open Systems,* Addison Wesley, 1996.
8. Hillston, J.E., King, P.J.B. y Pooley, R.J. (eds.), *Computer and Telecommunications Performance Engineering,* Londres: Springer Verlag, 1992.
9. McNamara, J.E., *Local Area Networks,* Bedford, MA: Digital Press, Educational Services, 1985.
10. Metcalfe, R.M. y Boggs, D.R., *Ethernet: Distributed Packet Switching for Local Computer Networks,* Comm. ACM 19, 7, 1976.
11. Miller, B.A. y Bisdikian, C., *Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications,* 2a. ed., Prentice Hall, 2001.
12. Norris, M., *Gigabit Ethernet Technology and Applications,* Artech House Publishers, 2002.
13. Perlman, R., *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols,* 2a. ed., Addison-Wesley Professional, 1999.
14. Peterson, L.L. y Davie, B.S., *Computer Networks: A Systems Approach,* 3a. ed., Morgan Kaufmann, 2003.
15. Riley, S. y Breyer, R., *Switched, Fast, and Gigabit Ethernet,* 3a. ed., Sams, 1998.
16. Ross, P.E., *FDDI-A Tutorial.* IEEE Communications Magazine, vol. 24, núm. 5, 1986.
17. Schwartz, M., *Telecommunications Networks — Protocols, Modeling and Analysis,* edición facsimilar, Addison Wesley, 1986.
18. Seifert, R., *Gigabit Ethernet: Technology and Applications for High-Speed LANs,* 1a. ed., Addison-Wesley Professional, 1998.
19. Seifert, R., *The Switch Book: The Complete Guide to LAN Switching Technology,* la. ed., Wiley, 2000.
20. Spurgeon, C.E., *Ethernet: The Definitive Guide,* O'Reilly, 2000.
21. Stallings, W., *Data and Computer Communications,* 6a. ed., Prentice Hall, 2004.
22. Stallings, W., *Wireless Communications and Networks,* Prentice Hall, 2002.

REFERENCIAS PARA LA PARTE IV

[RFC 751] Lebling, P., *Survey of FTP Mail and MLFL,* RFC 751, 1978.

[RFC 760] Postel, J., *DoD Standard Internet Protocol,* RFC 760, 1980.

[RFC 768] Postel, J., *User Datagram Protocol,* 1980.

[RFC 791] Postel, J., *Internet Protocol,* STD 5, RFC 791, 1981.

[RFC 792] Postel, J., *Internet Control Message Protocol,* 1981.

[RFC 793] Postel, J., *Transmission Control Protocol,* 1981.

[RFC 950] Mogul, J. y Postel, J., *Internet Standard Subnetting Procedure,* STD 5, RFC 950, 1985.

[RFC 1122] Braden, E.R., *Requirements for Internet Hosts-Communication Layers,* 1989.

[RFC 1349] Almquist, P., *Type of Service in the Internet Protocol Suite,* 1992.

[RFC 1517] Internet Engineering Steering Group and Hinden, R., *Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR),* RFC 1517, 1993.

[RFC 1518] Rekhter, Y. y Li, T., *An Architecture for IP Address Allocation with CIDR,* RFC 1518,1993.

[RFC 1519] Fuller, V., Li, T., Yu, J. y Varadhan, K., *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy,* RFC 1519, 1993.

[RFC 1520] Rekhter, Y. y Topolcic, C., *Exchanging Routing Information Across Provider Boundaries in the CIDR Environment,* RFC 1520, 1993.

[RFC 1700] Reynolds, J. y Postel, J., *Assigned Numbers,* 1994.

[RFC 1752] Bradner, S. y Mankin, A., *The Recommendation for the IP Next Generation Protocol,* RFC 1752, 1995.

[RFC 1878] Pummill, T. y Manning, B., *Variable Length Subnet Table For IPv4,* RFC 1878, 1995.

[RFC 2050] Hubbard, K., Kosters, M. y cols., *Internet Registry IP Allocation Guidelines,* BCP 12, RFC 2050, 1996.

[RFC 2131] Droms, R., *Dynamic Host Configuration Protocol,* RFC 2131, 1997.

[RFC 2132] Alexander, S. y Droms, R., *DHCP Options and BOOTP Vendor Extensions,* RFC 2132, 1997.

[RFC 2373] Hinden, R., *IP Version* 6 *Addressing Architecture,* RFC 2373, 1998.

[RFC 2460] Deering, S. y Hinden, R., *Internet Protocol, Version* 6 *(IPv6) Specification,* RFC 2460, 1998.

[RFC 2998] Bernet, Y., Ford, P. y cols., *A Framework for Integrated Services Operation over Diffserv Networks,* 2000.

[RFC 3232] Reynolds, J., *Assigned Numbers: RFC 1700 is Replaced by an On-line Database,* ed. 2002.

[RFC 3246] Davie, B., A. Charny, A. y cols., *An Expedited Forwarding PHB (Per-Hop Behavior),* 2002.

[RFC 3290] Bernet, Y., Blake, S. y cols., *An Informal Management Model for Diffserv Routers,* 2002.

[RFC 3513] Hinden, R. y Deering, S., *Internet Protocol Version* 6 *(IPv6) Addressing Architecture,* RFC 3513, 2003.

LECTURAS RECOMENDADAS PARA LA PARTE IV

1. Boney, J., *Cisco IOS in a Nutshell,* O'Reilly, 2001.
2. Coltun, R., *OSPF: An Internet Routing Protocol.* ConneXions: The Interoperability Report, vol. 3, núm. 8, 1989.
3. Comer, D.E., *Internetworking with TCP/IP,* vol. 1: *Principles, Protocols, and Architecture,* 3a. ed., Prentice Hall, 2000.
4. Davidson, J., *An lntroduction to TCP/IP,* Nueva York: Springer Verlag, 1992.
5. Feit, S., *Architecture, Protocols, and Implementation with IPv6 and IP Security,* McGraw-Hill, 1997.
6. Hunt, C., *TCP/IP Network Administration,* 2a. ed., O'Reilly, 1998.
7. Kleinrock, L., *Communication Nets: Stochastic Message Flow and Delay,* Nueva York: McGraw-Hill, 1964.
8. Kleinrock, L., *Queueing Systems,* vol. 2: *Computer Applications,* Nueva York: John Wiley & Sons, 1976.
9. Kleinrock, L., *Queueing Systems*, vol. 1: *Theory,* Wiley-Interscience, 1975.
10. Nogl, M., *Illustrated TCP/IP, A Graphic Guide to the Protocol Suite,* John Wiley & Sons, 1999.
11. Roberts, L.G., *Judgment Call,* revista informativa de comunicaciones, abril de 1999.
12. Shenker, S. y Partridge, C., *Specification of Guaranteed Quality of Service,* selección IETF, 1995.
13. Snader, J., *Effective TCP/IP Programming,* DMK Press, 2001.
14. Specification: *NetWare Link Services Protocol (NLSP),* revisión 0.9, número de parte 100-001708-001, 1993.
15. Stevens, W.R., *TCP/IP Illustrated,* vol. 1: *The Protocols,* 1a. ed., Addison-Wesley Professional, 1993.
16. Varghese, G., *Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices,* Morgan Kaufmann, 2004.

REFERENCIAS PARA LA PARTE V

[RFC 2514] Noto, M., Spiegel, E. y Tesink, K., *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management,* **ftp://ftp.isi.edu/in-notes/ rfc2514.txt**, 1999.

[RFC 2515] Tesink, K., *Definitions of Managed Objects for ATM Management,* **ftp://ftp.isi.edu/in-notes/rfc2515.txt**, 1999.

[RFC 2684] Grossman, D. y Heinanen, J., *Multiprotocol Encapsulation over ATM Adaptation Layer* 5, **ftp://ftp.isi.edu/in-notes/rfc2684.txt**, 1999.

[RFC 2761] Dunn, J. y Martin, C., *Terminology for ATM Benchmarking,* **ftp://ftp.isi.edu/in-notes/rfc276Ltxt**, 2000.

[RFC 2955] Rehbehn, K., Nicklass, O. y Mouradian, G., *Definitions of Managed Objects for Monitoring and Controlling the Frame Relay/ATM PVC Service Interworking Function,* **ftp://ftp.isi.edu/in-notes/rfc2955.txt**, 2000.

[RFC 3035] Davie, B., Lawrence, J. y cols., *MPLS using LDP and ATM VC Switching,* **ftp://ftp.isi.edu/in-notes/rfc3035.txt**, 2001.

[RFC 3116] Dunn, J. y Martin, C., *Methodology for ATM Benchmarking,* **ftp://ftp.isi.edu/in-notes/rfc3116.txt**, 2001.

[RFC 3134] Dunn, J. y Martin, C., *Terminology for ATM ABR Benchmarking,* **ftp://ftp.isi.edu/in-notes/rfc3134.txt**, 2001.

LECTURAS RECOMENDADAS PARA LA PARTE V

1. Aboba, B., NAT *and IPSEC* Internet Engineering Task Force, 2000.
2. *Advanced MPLS Design and Implementation,* Cisco Press, 2001.
3. Armitage, G., *Quality of Service in IP Networks,* Pearson Education, 2000.
4. Balaji, K., *Broadband Communications,* McGraw-Hill, 1998.
5. Berkowitz, H., *Requirements Taxonomy for Virtual Private Networks,* Internet Engineering Task Force, 1999.
6. *Big Book of Multiprotocol Label Switching RFC,* Morgan Kaufmann Publishers, 2000.
7. Black, U., *Internet Security Protocols: Protecting IP Traffic,* 1a. ed., Prentice Hall, 2000.
8. Black, U., *Emerging Communications Technologies,* 2a. ed., Prentice Hall Professional, 1997.
9. *Building Switched Networks: Multilayer Switching, QoS, IP Multicast, Network Policy, and Service Level Agreements,* 1a. ed., Addison-Wesley, 1999.
10. Busschbach, P.B., "Toward QoS-Capable Virtual Private Networks", *Bell Labs Technical Journal*, vol. 3, núm. 4, 1998.
11. Casey, L., *An Extended IP VPN Architecture,* Internet Engineering Task Force, 1998.
12. Dobrowski, G. y Grise, D., *ATM and Sonet Basics,* APDG Publishing, 2001.
13. Dutton, H. y Lenhard, P., *Asynchronous Transfer Mode (ATM) Technical Overview,* 2a. ed., Prentice Hall, 1995.
14. Feit, S., *Architecture, Protocols, and Implementation with IPv6 and IP Security,* McGraw-Hill, 1997.
15. Ford, W., *Computer Communications Security,* Prentice Hall, 1994.
16. Ginsburg, D., *ATM Solutions for Enterprise Internetworking,* 2a. ed., Addison-Wesley, 1998.
17. Gonsalves, M., *Voice Over IP Networks,* edición Bk & CD-Rom, McGraw-Hill Osborne Media, 1998.
18. Hunt, C., *TCP/IP Network Administration,* 2a. ed., O'Reilly, 1998.
19. Ibe, O.C., *Converged Network Architectures: Delivering Voice and Data Over IP, ATM, and Frame Relay,* Wiley, 2001.
20. Ibe, O.C., *Essentials of ATM Networks and Services,* Addison-Wesley, 1997.
21. Jamieson, D., Jamoussi, B. y cols., *MPLS VPN Architecture,* Internet Engineering Task Force, 1998.
22. Kompella, K. y cols., *MPLS-based Layer* 2 *VPN,* Internet Engineering Task Force, 2000.
23. Kurose, J. F. y Ross, K.W., *Computer Networking: A Top-Down Approach Featuring the Internet,* 3a. ed., Addison Wesley, 2004.
24. Li, T., *CPE based VPN using MPLS,* Internet Engineering Task Force, 1998.
25. McDysan, D.E. y Spohn, D.L., *ATM Theory and Applications,* McGraw Hill, 1998.
26. McDysan, D.E. y Spohn, D.L., *Hands-On ATM,* McGraw-Hill, 1998.
27. Morris, S., *Network Management, MIBs and MPLS: Principles, Design and Implementation,* Prentice Hall, 2003.
28. *MPLS and VPN Architectures,* vol. 1, Cisco Press, 2000.
29. *MPLS and VPN Architectures,* vol. 2, Cisco Press, 2003.
30. Muthukrishnan, K. y Malis, A., *Core MPLS IP VPN Architecture,* Internet Engineering Task Force, 2000.
31. Perros, H.G., *An Introduction to ATM Networks,* Wiley, enero de 2001.
32. Sackett, G.C. y Metz, C., *ATM and Multiprotocol Networking,* McGraw-Hill, 1997.

33. Siu, S. y Jain, R., *A Brief Overview of ATM: Protocol Layers, LAN Emulation and Traffic Management,* Computer Communications Review (ACM SIGCOMM), 1995.
34. Stanford, H., *Telecommunications for Managers,* 3a. ed., Prentice Hall, 1995.
35. Stevens, R.W., *TCP/IP Illustrated,* vols. 1-3, 1a. ed., Addison-Wesley Professional, 1993.
36. Sun, W., Bhaniramka, P. y Jain, R., *Quality of Service Using Traffic Engineering over MPLS: An Analysis*, Proc. 25th Annual IEEE Conference on Local Computer Networks (LCN 2000), Tampa, Florida, noviembre 8-10 de 2000.
37. *The MPLS Primer: An Introduction to Multiprotocol Label Switching,* Prentice Hall, 2001.
38. Thompson, R.A., *Telephone Switching Systems,* 1a. ed., Artech House Publishers, 2000.
39. Zorn, G., Pall, G. y cols., *Point-to-Point Tunneling Protocol (PPTP),* Internet Engineering Task Force, 1999.
40. Zwcky, E.D., Cooper, S. y Chapman, B.D., *Building Internet Firewalls,* O'Reilly, 2000.

ÍNDICE TEMÁTICO

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X